LES ENJEUX JURIDIQUES DE L'ANONYMAT SUR INTERNET

Michel Montazeau

Mémoire Master 2 – Droit du numérique Administration-Entreprise

Université Paris 1 Panthéon-Sorbonne

Sous la direction de M. Fabrice Mattatia

Je tiens à remercier l'ensemble de l'équipe pédagogique du Master, tout particulièrement Mme Irène Bouhadana et M. William Gilles qui le dirigent avec tant de passion. Je tiens à remercier M. Fabrice Mattatia pour sa disponibilité et son aide précieuse pour ce mémoire.

Je tiens à remercier mes parents pour leur soutien et leurs conseils, mon frère, mes très chères grands-mères et mes tantes pour leur amour inconditionnel ainsi que l'ensemble de ma famille.

Je tiens également à remercier Paul pour notre longue et riche amitié ainsi que mes amis Arthur, Alexandre P. et David pour nos débats juridiques ainsi qu'Alexandre K.

Enfin, j'ai une pensée toute particulière pour mes grands-pères et mon oncle qui me manquent.

Sommaire

Introduction

La pratique de l'anonymat s'est développée dès la littérature grecque antique de la fin du VIIIe siècle avant J.-C. Nombreux historiens débattent encore pour savoir si le poète grec Homère fut, comme cela a longtemps été considéré, une seule et même personne ou bien une entité construite. Le patronyme même de l'auteur de l'Iliade et de l'Odyssée n'est pas un vrai nom car il signifie « *l'otage* » ou « *celui qui est obligé de suivre* », ce qui révèle l'ancienne condition d'esclave de l'artiste. Il s'agit de la première forme connue de pseudonyme ou d'avatar. Quoi qu'il en soit, personnage historique ou fictif, Homère jouit toujours aujourd'hui d'une popularité et d'une postérité uniques dans la littérature mondiale dont nous aimons à penser qu'elle est aussi due au mystère qui entoure le poète.

Cette anecdote permet de souligner avant toute chose que l'anonymat a d'abord une connotation positive. A l'heure où le pouvoir politique se saisit de questions relatives à la neutralité des réseaux, et notamment celui d'Internet, la question de l'anonymat arrive au premier plan. Nadine Morano, ancienne secrétaire d'Etat et ministre, avait publiquement critiqué la pratique de l'anonymat sur le réseau social Twitter en considérant qu'il s'agissait en réalité de lâcheté[1], ouvrant de ce fait un débat sur un pilier de notre société, à savoir la liberté d'expression.

Comme nous le verrons, cette liberté n'est pas la seule implication de l'anonymat sur Internet. On peut en effet retrouver la notion à travers différentes dimensions. L'e-anonymat peut être par exemple un garant de la vie privée, droit fondamental reconnu par la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (CESDHLF) qui dispose en son article 8 que « *Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance* ». La Cour européenne des droits de l'homme avait d'ailleurs considéré dans une affaire *S. et Marper c. Royaume-Uni* de 2008 que

[1] Dom BOCHEL GUEGUAN, « Morano et l'anonymat sur Twitter : une nouvelle polémique pour rester dans la lumière », Le Nouvel Observateur, 5 juin 2012, [http://leplus.nouvelobs.com/contribution/565344-morano-et-l-anonymat-sur-twitter-une-polemique-pour-rester-dans-la-lumiere.html].

la « *protection des données personnelles joue un rôle fondamental dans l'exercice du droit au respect de la vie privée et familiale*[2] ». En l'espèce, il ne s'agissait pas de données personnelles en ligne mais d'empreintes digitales et génétiques conservées par les services de police britanniques. La formulation de cette phrase reste cependant assez large pour accueillir le maximum d'hypothèses et notamment celles des données personnelles sur Internet.

Revenons à la culture grecque. L'adjectif *anonyme* vient du vieil hellénique *anônumos* qui signifie « *sans nom* ». A vrai dire, le sens n'a pas beaucoup changé aujourd'hui. La définition donnée par le Littré est la suivante : « *Qui est sans nom* ». L'anonymat est donc avant tout un secret sur le nom, élément majeur si ce n'est principal de ce qui constitue dans l'esprit de chaque homme une identité. Le nom se transmet, indique l'appartenance à une famille, à un groupe social, à une origine et en d'autres temps à un corps de métier. Le *nom* a donc longtemps été le moyen exclusif de déterminer une *identité* et les deux notions peuvent encore être confondues aujourd'hui.

Mais la conception de l'identité a évolué. L'apparition de l'Internet public en août 1991 grâce à la mise à disposition du public de l'application « *WorldWideWeb* » a été le point de départ de cette mutation : c'est le moment où le citoyen connecté commence une nouvelle vie, une vie numérique. Le web, encore loin d'être régulé, est un nouvel espace de liberté. Au fur et à mesure que les sites web se multiplient, les pratiques se diversifient. Certaines sont nées à cette époque et sont toujours utilisées à l'heure actuelle comme les forums et les courriers électroniques. L'internaute peut désormais choisir un nouveau *nom* et créer une nouvelle *adresse* digitale. L'internaute, le citoyen, le parent, le bon père de famille, le majeur, le mineur, le commerçant, le consommateur, le juge, l'avocat, le délinquant, le fonctionnaire, l'élu, l'employeur, l'employé, le bailleur et le locataire disposent librement de deux notions fondamentales qui composent l'identité et peuvent ainsi se créer une *identité numérique*.

L'apparition du « *Web 2.0* » correspond à l'explosion des wiki, des blogs, du commerce en ligne et des réseaux sociaux. Ces nouvelles pratiques vont contribuer à l'enrichissement et au développement de l'identité numérique qui ne se compose plus seulement d'un *nom* et d'une *adresse* mais aussi de *contenus* (textes, images, sons, vidéos), *d'habitudes de consommation* et de *relations*. De plus, Internet ne permet pas seulement de se créer une

[2] CEDH, 4 décembre 2008, n° 30562/04 et 30562/04, *S. et Marper c. Royaume-Uni*, § 103.

nouvelle identité, mais plusieurs identités[3]. Bien sûr, beaucoup d'internautes retranscrivent leur identité traditionnelle sur Internet. Rien n'oblige à se créer un avatar ou un pseudonyme.

Dans le monde réel, personne ne tolère d'ingérence dans sa vie privée telle qu'elle peut se pratiquer sur Internet avec ou sans le consentement des personnes. Du fait de la volatilité de la notion d'identité numérique, du morcellement des données identifiantes et de la technicité de plus en plus croissante des applications informatiques et des algorithmes sur lesquels elles reposent, nous ne savons pas toujours grâce à quoi et par quel moyen nous pouvons être identifiés. C'est contre cette ingérence silencieuse que certaines personnes cherchent à se protéger en revendiquant un « *droit à l'anonymat* », c'est-à-dire un droit protecteur de la vie privée numérique, y compris chez les juristes les plus sérieux[4].

Ce constat souligne d'autant plus la spécificité d'Internet. Alors que personne ne s'oppose à l'inscription au registre d'Etat civil dès la naissance (prévue par l'article 55 du Code civil), les citoyens paraissent très sensibles à l'idée d'être identifiés sur les réseaux. Il s'agit là d'un paradoxe étrange qui peut s'expliquer par le caractère non maîtrisable d'Internet et, par extension, de la peur parfois irrationnelle que peuvent engendrer les nouvelles technologies.

Il existe une définition officielle du droit à l'anonymat. Le Groupe International de Travail sur la Protection des Données Personnelles dans les Télécommunications (GITPDPT) a adopté le 4 mars 2008 le « *Rome Memorandum* »[5] dont les orientations invitent les Etats à introduire le droit à l'anonymat défini comme « *le droit d'agir sur un service de réseautage social sous un pseudonyme sans avoir à révéler sa véritable identité aux autres utilisateurs, ou au public le plus large* »[6]. Même si cette définition place la question du droit à l'anonymat dans le contexte exclusif des réseaux sociaux et du droit au pseudonymat (plus restreint que le droit à l'anonymat) ou à l'hétéronymat, elle a le mérite d'institutionnaliser la question. Mais le GITPDPT n'est pas le seul à s'intéresser à la question. Dès 1999, le Comité des ministres du Conseil de l'Europe s'est inquiété de la protection de la vie privée sur Internet et a considéré que « *l'accès et l'utilisation anonyme des service* […] *constituent la meilleure*

[3] Ce qui renvoie à la notion d'hétéronymat.
[4] Groupe de travail TIC, *Déclaration des droits de l'homme numérique*, Mairie d'Issy-les-Moulineaux, Livre blanc d'André SANTINI et d'Alain BENSOUSSAN, 20 novembre 2000, pp. 18, 22, art. 6.
[5] Groupe international de travail sur la protection des données personnelles dans les télécommunications, *Report and guidance on privacy in social networks services* (Rapport et orientations sur la vie privée sur les réseaux sociaux) ou « *Rome Memorandum* », 4 mars 2008, 675.36.5, [http://www.datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdpt/working-papers-and-common-positions-adopted-by-the-working-group].
[6] *Idem*, p.10.

protection de la vie privée »[7]. Ces recommandations n'étant pas juridiquement contraignantes, nous estimons que la question est toujours en débat. L'objet du présent mémoire est justement d'essayer de déceler les principaux enjeux juridiques qu'implique l'anonymat sur Internet.

Les définitions doctrinales d'un droit à l'anonymat sont plus volatiles. L'anonymat peut être considéré comme une liberté civile, une liberté publique, un droit de la personnalité ou un droit subjectif qu'on peut rapprocher avec le droit à s'opposer à un traitement prévu à l'article 38 de la loi informatique et libertés du 6 janvier 1978. Le droit à l'anonymat est un droit en creux ou un droit en esquisse selon l'expression du professeur Beignier.

Mais quelles sont les manifestations de l'anonymat en dehors de la vie numérique ? Il est en effet possible de retrouver l'expression d'un tel droit au sein de différents régimes juridiques. Dans le droit de la famille, la procédure de l'accouchement sous X est ouverte par l'article 326 du Code civil qui dispose que « *Lors de l'accouchement, la mère peut demander que le secret de son admission et de son identité soit préservé* ». L'article L.222-6 du Code de l'action sociale et des familles prévoit quant à lui les conditions d'exercice de ce droit en détaillant les prérogatives de la mère de l'enfant. Dans ces hypothèses, la mère dispose librement du droit à voir son identité révélée. Cependant, dans certains cas clairement arrêtés par l'article L.147-6 du même code, l'identité de la mère ou du père pourra être communiquée par le Conseil national d'accès aux origines personnelles (CNAOP) aux personnes énumérées par l'article L.147-2. Mais même dans le cadre de l'article L.147-6 qui ouvre les cas de révélation d'identité des parents aux demandeurs, le consentement du père ou de la mère peut toujours faire obstruction à l'exercice du droit à connaître ses origines. Les positions morales sur ce droit à garder l'anonymat sur le lien de filiation peuvent varier. Cependant, le droit vient encadrer des réalités sociales tout en essayant d'équilibrer les rapports entre les droits en conflit. Dans ce cas là, c'est le consentement du parent, la personne anonyme, qui prévaut. Dans une décision « *Odière c. France* » rendue en 2003, la Cour Européenne des Droit de l'Homme (CEDH) a exprimé le rôle de régulateur social de ce droit à l'anonymat des parents en considérant que « *l'intérêt général est également en jeu dans la mesure où la loi française a pour objectif de protéger la santé de la mère et de l'enfant lors de l'accouchement, d'éviter des avortements en particulier clandestins et des abandons "sauvages". Le droit au respect de*

[7] Comité des ministres du Conseil de l'Europe sur la protection de la vie privée sur Internet, Annexe de la recommandation N° R (99) 5, 23 février 1999, II, 3° [https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=1897342&SecMode=1&DocId=396770&Usage=2].

la vie n'est ainsi pas étranger aux buts recherchés par le système français[8] ». Le droit à l'anonymat incarne ici un véritable régulateur propre à garantir l'intérêt général.

Dans le cadre du don d'organe, l'anonymat ne constitue pas un droit mais une obligation légale. Les articles 16-8 du Code civil[9] et l'article L.1211-5 du Code de la santé publique[10] posent en des termes presque identiques un principe d'interdiction de toute divulgation d'information sur l'identité receveur au donneur ou d'information sur l'identité du donneur au receveur. Cet anonymat ne peut être levé qu'en cas de nécessité thérapeutique.

Enfin, l'article L. 59 du Code électoral dispose tout simplement que « *Le scrutin est secret* ». L'action de voter est perçue en France comme l'expression de sa conscience politique. Afin d'inciter les citoyens à voter et à le faire librement, c'est à dire sans l'immixtion de tiers dans son choix, l'action de mettre le scrutin dans l'enveloppe se fait à l'abri des regards. De surcroît, la solennité est si poussée qu'un vote peut être refusé si le scrutin n'a pas été mis dans l'enveloppe dans les isoloirs prévus.

Dans la vie numérique, l'anonymisation des données effectuée dans un bref délai par un responsable de traitement le dispense de donner à la personne auprès de laquelle les données sont collectées certaines informations telles que le « *caractère obligatoire ou facultatif des réponses* », les « *destinataires ou catégories de destinataires des données* » et même des éventuels transferts de données vers un Etat tiers à l'Union Européenne (UE)[11]. L'anonymat est donc protecteur lorsqu'il permet de réduire les obligations des responsables de traitements. La loi informatique et libertés prévoit également un mécanisme d'anonymisation des données de santé en son article 8. Enfin, la CNIL peut émettre son avis sur un mécanisme d'anonymisation en vertu de l'article 11.

Ces dispositions n'embrassent cependant pas toutes les implications de l'anonymat sur Internet. En effet, il semble qu'une approche à la fois internationale, comparée et juridiquement globale s'impose lors de cette étude.

---

[8] CEDH, 13 février 2003, n° 42326/98, *Odièvre c. France.*

[9] « *Aucune information permettant d'identifier à la fois celui qui a fait don d'un élément ou d'un produit de son corps et celui qui l'a reçu ne peut être divulguée. Le donneur ne peut connaître l'identité du receveur ni le receveur celle du donneur* ».

[10] « *Le donneur ne peut connaître l'identité du receveur, ni le receveur celle du donneur. Aucune information permettant d'identifier à la fois celui qui a fait don d'un élément ou d'un produit de son corps et celui qui l'a reçu ne peut être divulguée* ».

[11] *Loi relative à l'informatique, aux fichiers et aux libertés*, n° 78-17, 6 janvier 1978, art. 32, IV.

D'abord, l'approche internationale se justifie car Internet n'a pas de frontières. Les Etats ont très vite compris que leurs droits internes ne suffiraient pas intervenir de manière pertinente et efficaces sur internet. A titre d'exemple, le Groupe « Article 29 », qui rassemble tous les homologues européens de la Commission Nationale Informatique et Libertés (CNIL) témoigne de ce besoin d'une réponse internationale.

Ensuite, il sera parfois nécessaire d'avoir une approche comparée car certains concepts émanant de systèmes juridiques différents nous aideront à mieux comprendre certains aspects de l'anonymat et notamment certains aspects de la vie privée.

Enfin, une approche juridiquement globale est indispensable afin de traiter juridiquement des enjeux de l'anonymat sur Internet. C'est l'autre particularité d'Internet d'avoir un impact sur toutes les matières du droit. Chaque ordre de juridiction a eu, à un moment ou à un autre, avoir à se prononcer sur des faits ou des règles de droit dans le contexte d'Internet. C'est pourquoi le présent mémoire comportera tant des décisions du juge constitutionnel que des décisions de la Cour de cassation et du Conseil d'Etat.

Il est aussi nécessaire, avant tout développement, de bien faire la différence entre droit à l'anonymat et droit à l'oubli. Le droit à l'oubli est théoriquement institué dans la loi informatique et libertés de 1978 au 5° de l'article 6 qui dispose que « *les données sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées* ». Il s'agit donc d'un droit correctif, c'est-à-dire qu'il s'exerce à posteriori de la collecte, volontaire ou non, d'informations. Le droit à l'anonymat aurait lui une vocation préventive de sorte que le droit à l'oubli n'aurait à être exercé que lorsque le droit à l'anonymat n'as pas été correctement exercé ou respecté.

Cependant les deux droits peuvent être rapprochés en deux points. Ils comprennent tous les deux la notion de vie privée[12]. Aussi, ces deux droits impliquent la notion d'identité. Le droit à l'anonymat cherche à en prévenir la collecte illégale ou la dénaturation et le droit à l'oubli cherche à en faire cesser le traitement.

Mais si la reconnaissance d'un droit à l'oubli est établie, notamment à travers le droit de rectification consacré à l'article 40 de la loi du 6 janvier 1978, il n'en est pas de même à

[12] Irène BOUHADANA, « Constitution et droit à l'oubli numérique : état des lieux et perspectives », Revue de l'Institut du monde et du développement, Les éditions IMODEV, 2011, p. 13.

propos du droit à l'anonymat. En effet, la reconnaissance d'un droit à l'anonymat n'est pas un sujet facile à arbitrer car il s'agit là de trancher sur l'équilibre entre les droits et libertés qui sont légitimement invocables par les citoyens et la nécessité de ne pas laisser se produire des comportements délinquants sur les réseaux avec une totale impunité pour leurs auteurs. De manière classique.

Ainsi, toute la réflexion autour de l'anonymat sera de soulever les différents enjeux juridiques afin de déterminer si l'anonymat est une notion effective et efficiente de notre système juridique.

Afin de répondre à cette question, il faudra d'abord déterminer les principaux enjeux qu'implique l'anonymat. La liberté d'expression a pris un nouvel essor en 2004 avec l'avènement d'un régime permettant la facilitation de la prise de parole en public sur Internet grâce à l'anonymisation conditionné de leur identité et coordonnées vis à vis des tiers. Impliquant également le droit au respect de la vie privée, notion mosaïque, il apparaît possible de déceler la trace d'un droit à l'anonymat par l'analyse des différentes règles visant à la prévention des atteintes à la vie privée (Partie 1). Cependant, si l'anonymat sur Internet peut paraître séduisant de prime abord, le principe n'est pas absolu et doit être tempéré par d'autres intérêts antagonistes, plus ou moins légitimes, ainsi que par la complexification des échanges sur Internet (Partie 2).

Partie 1. L'anonymat comme source de droits et libertés

L'anonymat est ce qu'on pourrait appeler un *droit en creux*, un droit qui transcende mais qui n'est pas exprimé. Comme nous l'avons déjà évoqué plus haut, la loi française consacre un droit à l'oubli à l'article 6, 5° de la loi informatique et libertés qui a vocation à s'exercer a posteriori mais aucun texte ne reconnaît explicitement de *droit à l'anonymat* sur les réseaux connectés qui serait effectif a priori de tout traitement.

D'une façon transcendantale, l'anonymat est la source de droits et libertés. La démocratisation d'Internet a vu le développement des *pages perso* puis des *blogs*. Depuis la LCEN de 2004, les internautes ont vu leur liberté d'expression prendre une tournure bien plus effective : la consécration d'un anonymat encadré par la loi est devenu un moyen de s'exprimer librement, bien évidemment dans le respect de la loi, sur un espace conférant une visibilité infinie. L'anonymat ainsi garanti a permis à une génération de citoyens internautes de s'exprimer, d'informer, de participer au débat public, de diversifier l'offre culturelle et de partager bien d'autres choses encore. Les critiques récurrentes sur la mauvaise qualité de l'information délivrée ou du manque de rigueur des blogueurs sont à notre avis sans objet : comme dans la presse traditionnelle (informative ou pas), un tri naturel se fait sur Internet. Les internautes induisent le trafic vers les sites et les blogs de qualité car, avant d'être internautes, ces personnes sont douées de raison et se dirige vers ce qui les nourrit intellectuellement en fonction de leurs besoins. L'anonymat de fait est devenu légal depuis 2004. Les personnes qui choisissent cette voie restent néanmoins responsables de leur contenu (Chapitre 1).

Mais dans le même temps, avec le développement des réseaux sociaux, du commerce électronique, du marché publicitaire sur le web ainsi que de la cybercriminalité et du cyber-terrorisme, la vie privée des internautes est devenue plus menacée. Le débat sur la vie privée numérique commence peu à peu à émerger et à intéresser les internautes. Cependant, la majorité d'entre eux n'ont pas conscience des données personnelles ou des traces qu'ils laissent sur les réseaux, en particulier sur le web, et qui sont susceptibles de porter préjudice à leur intimité (Chapitre 2).

A ces égards, un anonymat préventif et effectif permettrait de juguler cette hémorragie. C'est pourquoi nous essaierons de proposer un raisonnement dont la finalité est la reconnaissance d'un corpus de règles, dont certaines existent déjà, non sans évoquer les différentes dimensions de l'anonymat (Chapitre 3).

Chapitre 1. L'exercice de la liberté d'expression par l'encadrement de l'anonymat des internautes

La LCEN de 2004 est venue, avec quelque peu de retard, encadrer les activités numériques jusque là régies par la directive 2000/31/CE du 8 juin 2000 sur le commerce électronique (qu'elle transpose) ainsi que quelques dispositions de la directive 2002/58/CE du 12 juillet 2002 sur la protection de la vie privée dans le secteur des communications électroniques. Cette loi constitue réellement le régime général du droit applicable sur Internet : elle arrête une série de définition et fait entrer dans le vieux droit français de nouvelles notions flanquées de leur définition et, par-dessus tout, elle fixe les règles relatives à la responsabilité des acteurs sur Internet.

Loin d'être exclusivement occidentale[13], la question de l'articulation entre anonymat et liberté d'expression représente un réel enjeu de modernisation de nos démocraties modernes en ce qu'il répond à un besoin exprimé par la société civile. En revanche, ce droit doit nécessairement être encadré et limité afin de respecter les droits et libertés concurrents. A ce titre, le législateur est venu instituer un régime spécifique aux éditeurs de contenu non professionnels.

Ainsi, l'existence d'un droit à l'anonymat de l'expression existe d'autant plus que ce droit est tempéré dans certaines hypothèses et qu'il ne place pas son titulaire en situation d'impunité. C'est un droit dont l'usage rend responsable. Dans une démarche pédagogique, il sera d'abord traité du statut des hébergeurs de contenu, nécessaire préalable pour comprendre le droit à l'anonymat de l'expression (Section 1), puis il sera développé des avancées découlant de ce régime pour la société civile numérique (Section 2).

Section 1. Le statut des hébergeurs de contenu

La LCEN est venue répartir les responsabilités entres divers acteurs de la communication en ligne. C'est le très long article 6 de cette loi qui vient fixer ce régime. Pour cela, le législateur a d'abord défini ce que nous appelons dans le langage courant les fournisseurs d'accès Internet (FAI) définis à l'article 6- I- 1° tels que des « *personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne* ».

[13] Julien L., « La justice sud-coréenne juge l'anonymat indispensable à la liberté d'expression », Numerama, 24 août 2012, consulté le 12/05/2013, [http://www.numerama.com/magazine/23499-la-justice-sud-coreenne-juge-l-anonymat-indispensable-a-la-liberte-d-expression.html].

Au sens de l'article 6- I- 2°, les *hébergeurs de contenu* sont « *Les personnes physiques ou morales qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services* […] ». Ces derniers sont logiquement plus exposés en cas de recours pour faute civile ou faute pénale. Afin de remédier à ce réflexe des auteurs de recours, la loi leur a imposé des obligations relatives à l'identification des auteurs des contenus. Mais avant tout, le législateur européen et le législateur français ont institué un régime de responsabilité allégé pour les hébergeurs et les FAI, ce qui n'est pas sans conséquence sur l'effectivité du droit à l'anonymat des éditeurs de contenu non professionnels, autrement dit des blogueurs ou acteurs numériques qui jouent désormais un rôle majeur dans l'information au public[14].

Ces notions ainsi expliquées, il convient maintenant d'étudier quel type de responsabilité le législateur a instauré au bénéfice de ces intermédiaires (§1) et quelles sont les obligations qui leur ont été imposées (§2). Ensuite, nous détaillerons le régime de l'anonymat de l'expression instauré au bénéfice des éditeurs de contenu à titre non professionnel (§4) après avoir analysé la contrepartie de ce régime qui réside dans l'identification auprès de l'hébergeur (§3).

§1. La responsabilité allégée des hébergeurs et des fournisseurs d'accès

Le même article est venu préciser que « *Les personnes mentionnées aux 1 et 2 ne sont pas des producteurs au sens de l'article 93-3 de la loi n° 82-652 du 29 juillet 1982 sur la communication audiovisuelle*[15] ». Autrement dit, les FAI ainsi que les hébergeurs sont à l'abri de la qualification de producteur de contenu, qualification qui peut emporter la qualification *d'auteur principal*. L'auteur principal est la personne qui peut être poursuivie pour l'ensemble des infractions de presse prévues au chapitre IV de la loi du 29 juillet 1881 sur la liberté de la presse, parmi lesquels les provocations aux crimes et délits, les délits contre la chose publique et les délits contre les personnes.

Les raisons d'un tel régime dérogatoire des hébergeurs découle de la nécessité de favoriser et stimuler le développement de la communication numérique selon la philosophie

[14] On peut par exemple penser à Twitter qui est devenu en quelques années une plateforme incontournable pour les citoyens « lambda » ou même pour les journalistes et personnalités politiques.
[15] *Loi pour la confiance en l'économie numérique*, n° 2004-575, 24 juin 2004, art. 6, I al. 6.

de la directive du 8 juin 2000 qui les qualifie d' « *intermédiaires techniques* »[16] parmi lesquels figure les hébergeurs. La directive dispose que les personnes concernées sont les opérateurs fournissant un simple transport[17] ou assurant une forme de stockage dite « *caching* »[18] ou proposant l'hébergement. Ces personnes ne sont donc pas tenues à une « *obligation générale en matière de surveillance* »[19]. En principe, la responsabilité dérogatoire de ces prestataires de service est donc une responsabilité allégée car elle ne pourra être déclenchée seulement s'ils ont été préalablement avertis du contenu illicite qu'ils stockent ou qu'ils transportent[20]. Autrement dit, depuis la LCEN, les hébergeurs n'ont pas d'obligation légale de vérifier ce contenu a priori mais la loi leur impose une réaction a posteriori après le signalement d'un contenu illicite (diffamation, injure, contrefaçon, trouble à l'ordre public).

C'est donc conformément à la directive que l'article 6- I- 2° de la loi du 21 juin 2004 dispose que « *Les personnes physiques ou morales qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services ne peuvent pas voir leur responsabilité civile engagée du fait des activités ou des informations stockées à la demande d'un destinataire de ces services si elles n'avaient pas effectivement connaissance de leur caractère illicite ou de faits et circonstances faisant apparaître ce caractère ou si, dès le moment où elles en ont eu cette connaissance, elles ont agi promptement pour retirer ces données ou en rendre l'accès impossible* […] ».

On retrouve également les préconisations de la directive à l'article 6- I- 7° de la même loi : « *Les personnes mentionnées aux 1 et 2 ne sont pas soumises à une obligation générale de surveiller les informations qu'elles transmettent ou stockent, ni à une obligation générale de rechercher des faits ou des circonstances révélant des activités illicites* […] ».

[16] P. DE CANDE, « La responsabilité des intermédiaires de l'internet ou ISP : l'apport du projet de loi sur la société de l'information », *D.* 2001, chron., p. 1934 ; J. R. REIDENBERG, « L'affaire Yahoo ! Et la démocratisation internationale », *CCE* 2001, étude n° 12.

[17] NB : la notion de transport est relative aux FAI, qui sont donc soumis à ce texte.

[18] En français : « mise en mémoire ».

[19] *Directive du Parlement européen et du Conseil relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur* (« *directive sur le commerce électronique* »), 8 juin 2000, 2000/31/CE, art. 12, art. 13, art. 14, art. 15.

[20] Une exception est posée par l'article 6, I, 7 alinéa 2 de la loi du 21 juin 2004 : « *Le précédent alinéa (celui sur la responsabilité allégée) est sans préjudice de toute activité de surveillance ciblée et temporaire demandée par l'autorité judiciaire* ».

§2. L'obligation de réagir « promptement »

La loi du 21 juin 2004 a cependant instauré une contrepartie aux bénéficiaires de la responsabilité allégée. Selon les articles 6- I- 2° et 6- I- 3° (qui concernent respectivement l'engagement des responsabilités civiles et pénales), l'hébergeur est tenu de réagir promptement lorsqu'il est averti du caractère illicite d'un contenu. L'alerte du caractère illicite peut être le fait d'un particulier ou d'une injonction judiciaire.

Agir promptement signifie, selon les deux articles, « *retirer* » ou « *rendre l'accès impossible* » aux données ou informations en cause. Il y a en réalité deux sortes de circonstances qui peuvent se présenter [21] : soit le contenu est manifestement illicite (provocation à la haine, à la violence ou à la discrimination, contestation de crimes contre l'humanité[22], apologie de crimes de guerre etc.) et l'hébergeur devra promptement retirer le contenu en cause ou rendre son accès au public impossible, soit le contenu n'est pas manifestement illicite (atteinte à la vie privée, contrefaçon) et l'hébergeur devra avertir promptement le fournisseur du contenu du problème, le sommer de réagir et de se mettre en contact avec le plaignant pour que soit apporté une solution au différend.

Aussi, le législateur a rendu obligatoires pour les hébergeurs les dispositifs de signalement de contenus illicites. L'article 6- I- 7° de la LCEN dispose « [Au titre de l'intérêt général attaché à la répression de l'apologie des crimes contre l'humanité, de l'incitation à la haine raciale ainsi que de la pornographie enfantine, les hébergeurs] *doivent mettre en place un dispositif facilement accessible et visible permettant à toute personne de porter à leur connaissance ce type de données* ».

De plus, il est instauré une présomption de connaissance de contenu illicite de la part de l'hébergeur lorsque leur est notifié, conformément à l'article 6- I- 5°, les éléments suivants :

> « *- la date de la notification ;*
> *- si le notifiant est une personne physique : ses nom, prénoms, profession, domicile, nationalité, date et lieu de naissance ; si le requérant est une personne morale : sa forme, sa dénomination, son siège social et l'organe qui la représente légalement ;*
> *- les nom et domicile du destinataire ou, s'il s'agit d'une personne morale, sa*

[21] Jérôme HUET, Emmanuel DREYER, *Droit de la communication numérique*, LGDJ, 2011, p. 121.
[22] Tout ce qui relève, par exemple, de la loi « Gayssot » n°90-615 du 13 juillet 1990.

dénomination et son siège social ;

- la description des faits litigieux et leur localisation précise ;

- les motifs pour lesquels le contenu doit être retiré, comprenant la mention des dispositions légales et des justifications de faits ;

- la copie de la correspondance adressée à l'auteur ou à l'éditeur des informations ou activités litigieuses demandant leur interruption, leur retrait ou leur modification, ou la justification de ce que l'auteur ou l'éditeur n'a pu être contacté. »

Ce recours offert au tiers suppose donc que ce dernier ait au préalable tenté de contacter le véritable responsable du contenu. Ainsi, cette procédure instaure un rapport de loyauté car cette démarche instaure la présomption que le responsable du contenu sera en position de supposer que des démarches ultérieures à son encontre pourront être exercées.

§3. L'identification des internautes

Conformément à ce que préconisait la directive du 8 juin 2000 en son article 15- 2°[23], l'article 6- II de la loi du 21 juin 2004 a prévu l'obligation pour les fournisseurs d'accès et les hébergeurs de détenir et de conserver « *les données de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont elles sont prestataires.* » Ces données peuvent en outre être demandées aux fournisseurs d'accès ou aux hébergeurs par l'autorité judiciaire[24]. Cette obligation est la contrepartie de la dispense d'obligation générale de surveillance faite aux hébergeurs et fournisseurs d'accès[25].

Le décret n°2011-219 du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne est venu préciser les données mentionnées par l'article 6- II

[23] « *Les États membres peuvent instaurer, pour les prestataires de services de la société de l'information, l'obligation d'informer promptement les autorités publiques compétentes d'activités illicites alléguées qu'exerceraient les destinataires de leurs services ou d'informations illicites alléguées que ces derniers fourniraient ou de communiquer aux autorités compétentes, à leur demande, les informations permettant d'identifier les destinataires de leurs services avec lesquels ils ont conclu un accord d'hébergement* ».

[24] La loi n°006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers a étendu ce pouvoir de réquisition aux agents de police et de gendarmerie chargés des missions de lutte contre le terrorisme sous le contrôle de la personnalité qualifiée instituée par l'article L. 34-1-1 du Code des postes et des communications électroniques et de la Commission nationale de contrôle des interceptions de sécurité. Ces données sont limitées « *aux données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques, au recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée, aux données relatives à la localisation des équipements terminaux utilisés ainsi qu'aux données techniques relatives aux communications d'un abonné portant sur la liste des numéros appelés et appelants, la durée et la date des communications* » en vertu du même article.

[25] Jérôme HUET, Emmanuel DREYER, *Droit de la communication numérique*, LGDJ, 2011, p. 132.

de la LCEN. Concernant les FAI, pour chaque connexion de leurs abonnés, ces données sont : l'identification de la connexion, l'identifiant attribué par le FAI à l'abonné, l'identifiant du terminal utilisé pour la connexion (lorsqu'ils y ont accès), les dates et heures de début et de fin de la connexion et les caractéristiques de la ligne de l'abonné. Les fournisseurs d'hébergement doivent quant à eux détenir et conserver, pour chaque opération de création : l'identifiant de la connexion à l'origine de la communication, l'identifiant attribué par le système d'information au contenu, les types de protocoles utilisés pour la connexion au service et pour le transfert des contenus, la nature de l'opération, les dates et heures de l'opération et enfin l'identifiant utilisé par l'auteur de l'opération lorsque celui-ci l'a fourni.

Ces données peuvent être sans mal considérées comme des données à caractère personnel au sens de l'article 2 de la loi informatique et libertés du 6 janvier 1978. Cette affirmation est dans la logique de la position de la CNIL qui considère que l'adresse IP est une donnée à caractère personnel[26] a l'instar du groupe « Article 29 »[27] et de certaines juridictions nationales[28], bien que la Cour d'Appel de Paris ait à deux reprises décidé du contraire[29]. Par extension, nous considérons donc que les données mentionnées sont des données à caractère personnel au sens du droit français tant elles présentent des caractéristiques proches de l'adresse IP. Cela explique donc l'encadrement dont elles font l'objet.

§4. Le régime de l'anonymat des éditeurs de contenu non professionnels

Tout d'abord, l'article 6- III- 2° alinéa 1 de la LCEN dispose que « *Les personnes éditant à titre non professionnel un service de communication au public en ligne peuvent ne tenir à la disposition du public, pour préserver leur anonymat, que le nom, la dénomination ou la raison sociale et l'adresse du prestataire mentionné au 2 du I* [les hébergeurs], *sous réserve de lui avoir communiqué les éléments d'identification personnelle prévus au 1*. » A la différence des données d'identification en cause dans le décret n°2011-219 du 25 février 2011

[26] CNIL, « L'adresse IP est une donnée à caractère personnel pour l'ensemble des CNIL européennes », 2 août 2007, [http://www.cnil.fr/linstitution/actualite/article/article/ladresse-ip-est-une-donnee-a-caractere-personnel-pour-lensemble-des-cnil-europeennes/].

[27] Groupe « Article 29 », *Avis sur le concept de données à caractère personnel*, 20 juin 2007.

[28] TGI Bobigny, 14 décembre 2006, *Laurent F. c/ Sacem et autres* ; TGI Paris, ord. , 24 décembre 2007, *Techland c/ France Telecom et autres*.

[29] C.A. Paris 13ème chambre, section B, 27 avril 2007, *G. c/ Ministère Public* ; CA Paris 13ème chambre, section A, 15 mai 2007, *S. c/ Ministère Public et autres*.

qui ne sont consultables que par « *les autorités publiques compétentes* »[30], ces éléments d'identification sont destinés au public. Cette protection des tiers civils est une réelle avancée pour la liberté d'expression ainsi que pour la protection de la vie privée.

Aussi, l'alinéa 2 du même article soumet les hébergeurs au secret professionnel dans les conditions prévues aux articles 226-13 et 226-14 du Code pénal « *pour tout ce qui concerne la divulgation de ces éléments d'identification personnelle ou de toute information permettant d'identifier la personne concernée*. » On voit ainsi que l'anonymat bénéficie de garanties sérieuses car la divulgation des données en cause encoure une qualification pénale, induisant une conduite irréprochable des hébergeurs. Toutefois, selon le même article, ce secret professionnel n'est pas opposable à l'autorité judiciaire.

De plus, le législateur est venu protéger les éditeurs de contenu, professionnels ou non, des signalements de contenu illicite abusifs ou dilatoires des tiers en instituant une peine d'emprisonnement d'un an et de 15000 euros d'amende[31].

Enfin, l'article 3 du décret du 25 février 2011, codifié à l'article L. 34-1- II du Code des Postes et des Communications Electroniques, fixe un délai de conservation des données de trafic des titulaires d'abonnements à un service de télécommunication et celles relatives aux « *opérations de création*[32] » des clients d'hébergeurs d'un an à compter du jour de la création des contenus. C'est un délai relativement court qui va dans le sens d'un droit à l'anonymat et arrêté conformément aux recommandations du groupe de travail « *Article 29*[33] ».

Ainsi est encadré l'anonymat des éditeurs de contenu à titre non professionnel. Il peut paraître paradoxal de considérer qu'un droit à l'anonymat de l'expression existe quand on se rend compte du cadre législatif détaillé qui l'entoure.

Cependant, si l'anonymat des éditeurs non professionnels ne peut être levée que sur réquisition de l'autorité judiciaire, cette garantie semble satisfaisante car, faut-il le rappeler, en vertu de l'article 66 de la Constitution du 4 octobre 1958, « *L'autorité judiciaire, gardienne*

[30] *Directive du Parlement européen et du Conseil relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur* (« *directive sur le commerce électronique* »), 8 juin 2000, 2000/31/CE, art. 15, 2°.
[31] *Loi pour la confiance en l'économie numérique*, 21 juin 2004, n°2004-575, art. 6, I, 4°.
[32] Les opérations de création sont définies à l'article 2 du décret n° 2011-219 du 25 février 2011 telles que « *des créations initiales de contenu* », « *des modifications des contenus et de données liées aux contenus* » et « *des suppressions de contenus* ».
[33] Groupe de travail « Article 29 », *Avis 5/2009 sur les réseaux sociaux en ligne*, WP 163, 12 juin 2009.

de la liberté individuelle, assure le respect de ce principe dans les conditions prévues par la loi. » De plus, nous préférons admettre que l'existence d'un droit se manifeste aussi par l'existence de conditions et de limites, comme par exemple le droit de réponse des personnes visées par un contenu[34]. Selon cette logique, le droit à l'anonymat de l'expression est un prolongement de la liberté d'expression.

Section 2. Les apports du droit à l'anonymat de l'expression à la société civile numérique

Il s'agira ici de présenter en quoi ce régime a bénéficier au développement d'une nouvelle forme de liberté (§1) et d'un des nouveaux moyen de l'exercer : le pseudonymat (§2).

§1. La liberté d'expression 2.0

En vertu de l'article 1 de la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication dite « loi Léotard », modifié par l'article 1 de la LCEN, « *La communication par voie électronique et libre* ». Les alinéas suivants rappellent toutefois que l'exercice de cette liberté est limité « *d'une part, par le respect de la dignité de la personne humaine, de la liberté et de la propriété d'autrui, du caractère pluraliste de l'expression des courants de pensée et d'opinion et, d'autre part, par la protection de l'enfance et de l'adolescence, par la sauvegarde de l'ordre public, par les besoins de la défense nationale, par les exigences de service public, par les contraintes techniques inhérentes aux moyens de communication, ainsi que par la nécessité, pour les services audiovisuels, de développer la production audiovisuelle*. »

Mais la liberté de communication instaurée par le législateur trouve son sens à la lecture de l'article 2 de la loi Léotard. La communication au public par voie électronique se définit comme « *toute mise à disposition du public ou de catégories de public, par un procédé de communication électronique, de signes, de signaux, d'écrits, d'images, de sons ou de messages de toute nature qui n'ont pas le caractère d'une correspondance privée*. » Cette définition trouve son écho dans le IV de l'article 1 de la LCEN. Cela traduit donc deux choses. La première est que le législateur a souhaité cette redondance afin d'établir durablement cette liberté. La seconde est que le législateur a voulu signifier sans équivoque

[34] *Loi pour la confiance en l'économie numérique*, 21 juin 2004, n°2004-575, art. 6, IV, al. 2.

que toute disposition de la LCEN de 2004 devra être interprétée à la lumière de cette liberté, liant ainsi à minima l'appréciation souveraine du juge.

La liberté de communication par voie électronique est-elle toutefois une nouvelle liberté ou le prolongement d'une liberté préexistante ? Selon notre avis, il s'agit du prolongement de la liberté d'opinion et d'expression, un renouvellement. A l'heure où cette expression se manifeste à travers le web, la lecture de l'article 19 de la Déclaration Universelle des Droits de l'Homme (DUDH) du 10 décembre 1948 qui dispose que « *Tout individu a droit à la liberté d'opinion et d'expression, ce qui implique le droit de ne pas être inquiété pour ses opinions et celui de chercher, de recevoir et de répandre, sans considérations de frontières, les informations et les idées par quelque moyen d'expression que ce soit* » trouve pleinement son sens car aucun autre moyen qu'Internet ne permet l'exercice de cette liberté pour chaque individu « *sans considération de frontières* ». Le même raisonnement peut ainsi s'opérer à propos de l'article 10, 1 de la CESDHLF[35].

En droit interne, la liberté d'opinion et d'expression est garantie par les articles 10 et 11 de la Déclaration des Droits de l'Homme et du Citoyen de 1789. Il en résulte que cette liberté s'exerce dans les limites fixées par la loi, car elle n'est ni générale, ni absolue[36]. Toutefois, les atteintes portées à l'exercice de cette liberté doivent être nécessaires, adaptées et proportionnées à l'objectif poursuivi[37].

Le juge constitutionnel, à travers plusieurs décisions, a fait évoluer la conception traditionnelle de la liberté d'opinion et d'expression par le prisme de la notion de liberté de communication en ligne. A l'occasion de l'examen de la loi n° 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet, le Conseil Constitutionnel a pu considérer qu' « *en l'état actuel des moyens de communication et eu égard au développement généralisé des services de communication au public en ligne ainsi qu'à l'importance prise par ces services pour la participation à la vie démocratique et l'expression des idées et des opinions, ce droit implique la liberté d'accéder à ces services*[38] ». Autrement dit, la liberté d'opinion et d'expression implique une autre liberté, celle d'accéder à des

[35] « *Toute personne a droit à la liberté d'expression. Ce droit comprend la liberté d'opinion et la liberté de recevoir ou de communiquer des informations ou des idées sans qu'il puisse y avoir ingérence d'autorités publiques et sans considération de frontière. Le présent article n'empêche pas les Etats de soumettre les entreprises de radiodiffusion, de cinéma ou de télévision à un régime d'autorisations.* »

[36] Cons. const., 27 juil. 1982, n° 82-141 DC, *Loi sur la communication audiovisuelle*, cons. 13.

[37] Cons. const., 10 juin 2009, n° 2009-580 DC, *Loi favorisant la diffusion et la protection de la création sur interne***,** cons. 15.

[38] Cons. const., 10 juin 2009, n° 2009-580 DC, *Loi favorisant la diffusion et la protection de la création sur interne*, cons. 12.

services de communication en ligne. La seule limite reconnue par le Conseil est relative aux contenus pédopornographiques[39].

L'anonymat des éditeurs non professionnels de contenu apparaît comme un support de cette liberté de communication en ligne. Cette « *liberté 2.0* » permet en effet aux membres de la société civile de franchir le pas de la publication de leurs opinions, de leurs analyses et de leurs créations. Le choix de l'anonymat n'est pas aveu de lâcheté mais l'expression de la volonté de protéger sa vie privée et ainsi de se mettre à l'abri des pressions des tiers. Les critiques classiques émises à l'encontre de l'anonymat des blogueurs ou de certains utilisateurs de Twitter ou de Youtube reposent en fait sur une mauvaise connaissance de la loi, notamment du régime instauré par la LCEN. Ce droit est d'autant plus fort et d'autant plus légitime qu'il n'est pas absolu car il trouve sa limite dans les droits et libertés énoncés, dans deux textes différents et dans les mêmes termes, à l'article 1, IV alinéa 2 de la loi du 21 juin 2004 ainsi qu'à l'article 1 alinéa 2 de la loi Léotard relative à la liberté de communication. Ainsi, les éditeurs anonymes ne sont pas en situation d'impunité, contrairement à ce qui peut être dit. A vrai dire, pour certains blogueurs, l'anonymat permet même de respecter leurs obligations déontologiques[40]. Aussi, faut-il rappeler que dans certains Etats dans lesquels la société civile appelle à une identique conception de notre liberté d'expression, l'anonymat est un moyen de résistance face à la censure et un moyen de relayer l'information contradictoire. Le plus bel exemple est sans doute incarné par Zhou Shuguang, blogueur chinois subversif ayant écrit sous le pseudonyme de « Zola » et qui est depuis 2008 assigné à ne pas sortir en dehors de sa ville natale.

Une fois que le droit à l'anonymat de l'expression est institué et assorti de garanties et de limites, ils convient de s'intéresser au principal moyen permettant de l'exercer.

§2. Le droit au pseudonyme : la croisée des chemins entre liberté d'expression et droit au respect de la vie privée

Un pseudonyme est un nom d'emprunt sous lequel une personne se fait connaître du public. Il a longtemps été l'apanage des artistes. Beaucoup pseudonymes sont passés à la postérité, qu'ils désignent des écrivains (Homère, François Rabelais, Balzac, Voltaire, Céline,

[39] Cons. const., 10 mars 2011, n° 2011-625 DC, *Loi d'orientation et de programmation pour la performance de la sécurité intérieure***,** cons. 8.
[40] Par exemple, le célèbre blog « Journal d'un avocat » tenu et mis à jour par Maître Eolas (pseudonyme), exerçant la profession d'avocat ainsi que d'autres professionnels du droit (notamment des magistrats). Voir aussi le blog de Maître Mô (pseudonyme).

Emile Ajar) ou encore des hommes de guerre (Colonel Fabien, Capitaine Stéphane, Chaban, Rol). La démocratisation du web a engendré une massification des pseudonymes : d'abord s'exprimant sous la forme du *log in*[41], la notion de pseudonyme, intrinsèquement liée à Internet[42], a muté sous la forme de noms d'utilisateurs personnalisables à l'infini.

Dans la vie réelle, le recours au pseudonyme n'est pas illicite. C'est au contraire une liberté qui n'est pas absolue. Par exemple, on ne peut choisir un pseudonyme de manière frauduleuse, par exemple, afin de porter atteinte au droit des tiers[43] ou aux bonnes mœurs[44]. Il a également été jugé que la révélation d'un pseudonyme porte atteinte à la vie privée[45]. Ce droit ne place pas le titulaire du pseudonyme en situation d'impunité. Par exemple, lorsqu'un pseudonyme a été un instrument de la commission d'une escroquerie, il peut être assimilé à un faux nom au sens de l'article 313-1 du Code pénal[46]. Aussi, l'utilisation d'un pseudonyme ne peut protéger contre des poursuites pour publicité illicite[47].

Le Code de la propriété intellectuelle (CPI) reconnaît également un droit pour les auteurs anonymes ou sous pseudonymes de jouir des droits prévus à l'article L.111-1 du CPI[48]. En d'autres termes, les auteurs ayant choisi de se dissimuler sous pseudonyme ou derrière l'anonymat ont les mêmes droits, qu'ils soient moraux ou patrimoniaux, que les auteurs ayant signé leurs œuvres de leur nom officiel. Aussi, l'article L.711-1 du CPI ouvre la possibilité de déposer un pseudonyme en tant que marque à l'Institut national de la propriété industrielle. Le droit au pseudonyme peut donc être un patrimonial et monopolistique.

Nous le disions dans notre introduction, la question du recours au pseudonyme sur les réseaux a été institutionnalisée. Dès 1997, le groupe « Article 29 » a pu à propos des blogs approuver l'usage des pseudonymes sous réserve de l'identification auprès des fournisseurs de service[49]. Le Comité des ministres du Conseil de l'Europe, à propos des services de réseautage social, a ainsi émis plusieurs recommandations dont certaines traitent du droit à recourir à un pseudonyme : « « *Le droit d'utiliser un pseudonyme devrait être garanti à la fois au regard de la liberté d'expression et du droit de communiquer et de recevoir des*

[41] En français : « identifiant de connexion ».
[42] Guillaume DESGENS-PASANAU, Eric FREYSSINET, *L'identité à l'ère du numérique*, 2009, Dalloz, p. 56.
[43] Civ. 1re, 19 juin 1961, D. 1961. 544 ; JCP 1961. II. 12298, note P. N.
[44] Crim. 17 nov. 1992, Bull. crim., no 379.
[45] TGI Paris, Ch. 1 sect. 1, 22 octobre 1997, Juris-Data 1997-047626.
[46] Crim. 27 oct. 1999, no 98-86.017, Bull. crim., no 235.
[47] Crim. 7 oct. 1992, no 91-12.845.
[48] *Code de la propriété intellectuelle*, art. L.113-6 al. 1.
[49] Groupe de travail « *Article 29* », *Recommandation 3/97, L'anonymat sur Internet*, WP 6, 3 décembre 1997, p. 9.

informations et des idées, et du droit au respect de la vie privée »[50]. Pour autant, « *cela n'empêche pas* […] *les autorités chargées de l'application de la loi d'avoir accès à la véritable identité d'un internaute lorsque cela s'avère nécessaire et sous la réserve de conformité aux garanties juridiques appropriées garantissant le respect des droits et des libertés fondamentales.* »[51] Le pseudonyme apparaît ici comme un moyen à part entière de préserver les droits garantis par la CESDHLF. Même si ces recommandations n'ont pas de valeur juridique contraignante, « *elles constituent un idéal à atteindre dont la Cour Européenne des Droits de l'Homme s'inspire pour faire évoluer sa jurisprudence* »[52].

Le droit au pseudonyme ainsi institutionnalisé est néanmoins toujours en débat car non inscrit dans loi au bénéfice de tout le monde. A ce titre, il n'est pas un droit effectif mais un droit en puissance. Il est vrai que, contractuellement, sur certains réseaux sociaux, l'usage d'un pseudonyme est en principe interdit[53] même si, fin 2012, un land allemand du Schleswig-Holstein a menacé d'attaquer Facebook en justice pour ce motif[54]. Il constitue en outre un élément majeur de la reconnaissance d'un réel droit à l'anonymat en ce qu'il permet l'exercice de la liberté d'expression numérique et du droit à l'identité.

[50] Conseil de l'Europe, Comité des ministres, *Recommandation du Comité des Ministres aux Etats membres sur la protection des droits de l'homme dans le cadre des services de réseaux sociaux*, CM/rec(2012)4, 4 avril 2012, p. 3.
[51] *Ibid*.
[52] Ludovic PAILLER, *Les réseaux sociaux sur internet et le droit au respect de la vie privée*, Larcier, 2012, p. 61.
[53] *Idem*, pp. 56-60.
[54] Ben ROONEY, « The debate over online anonymity », *Tech-europe, The Wall Street Journal*, 17 jan. 2013, [http://blogs.wsj.com/tech-europe/2013/01/17/the-debate-over-online-anonymity/].

Chapitre 2. Les rapports entre anonymat et vie privée sur Internet

Le respect de la vie privée fait partie des droits les plus encadrés tant par le droit international que par le droit interne. Cependant, avant toute analyse juridique, il convient de s'intéresser aux concepts qui composent la vie privée (Section 1) avant de replacer la notion de vie privée dans le paradigme d'Internet (Section 2).

Section 1. Les trois dimensions d'une vie privée en question

Dans les sociétés démocratiques, le droit au respect de la vie privée est une garantie contre toute ingérence dans son intimité et apparaît comme un droit pilier. Ce sentiment fut assez bien résumé par l'avocat et membre de la Cour Suprême des Etats-Unis Louis Brandeis qui en 1928 évoquait « *the right to be left alone*[55] » : « *Ceux qui ont rédigé notre Constitution entendaient sécuriser les conditions favorables à la poursuite du bonheur. Ils reconnaissaient l'aspect spirituel de la nature humaine, de ses sentiments et de son intelligence. Ils savaient que seulement une part des peines, plaisirs et satisfactions de la vie sont à trouver dans les choses matérielles. Ils cherchaient à protéger les Américains dans leurs croyances, leurs pensées, leurs émotions et leurs sensations. Ils ont donné contre le gouvernement le droit d'être laissé seul – le plus étendu des droits et le plus estimé pour les êtres civilisés*[56] ».

Cette déclaration permet d'introduire de manière très générale, mais néanmoins juste, la vision contemporaine de la vie privée. Cependant, une approche décortiquée s'impose dans notre démarche scientifique afin de couvrir la totalité du spectre de la vie privée.

Dans son ouvrage « *Economie des données personnelles* », Fabrice Rochelandet considère 3 dimensions de la vie privée[57] : le secret (§1), la tranquillité (§2) et l'autonomie individuelle (§3). Ces trois dimensions de la vie privée seront utiles pour les développements ultérieurs.

§ 1. Le secret

Dans cette dimension, l'individu est libre de choisir en ce qui le concerne le temps, les circonstances et la mesure dans lesquelles ses attitudes, ses croyances, ses comportements et ses opinions doivent être partagés avec ou cachés des autres. C'est donc l'autonomie de la volonté qui est placée au premier plan. Cette dimension est particulièrement intéressante car il

[55] En français : « le droit d'être laissé seul ».
[56] Louis BRANDEIS, 4 juin 1928, *Olmstead c. Etats-Unis (Olmstead v. United-States).*
[57] Fabrice ROCHELANDET, *Economie des données personnelles*, La Découverte, 2010, pp. 8-10.

est aisé de constater que dans la vie numérique de tout les jours, c'est-à-dire les échanges commerciaux et sociaux mais encore les requêtes sur les moteurs de recherche, l'autonomie de la volonté est indiscutablement remise en cause.

Google a récemment mis en place un petit encart permettant d'informer ses utilisateurs sur l'utilisation faite de leur « *cookies* »[58] afin de se conformer aux prescriptions de l'article 5 de la directive 2002/58 du 12 juillet 2002 du Parlement Européen selon lequel une information claire et complète doit être délivrée à l'utilisateur quant à la finalité du traitement opéré sur ses données personnelles ainsi qu'aux dispositions de l'article 6 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés selon lesquelles les données personnelles doivent être collectées pour des finalités déterminées, explicites et légitimes. Dans les faits, le géant de Mountain View se contente d'une information complètement illisible pour l'utilisateur moyen, procédant ainsi à une exploitation de l'ignorance scandaleuse. La procédure à suivre afin de désactiver l'enregistrement intempestif des cookies devrait aussi être facilitée, par exemple, avec un autre encart bien visible.

En somme, c'est une dimension de la vie privée qui est souvent violée car le consentement des utilisateurs, quand il est recueilli, ne peut être considéré comme libre et éclairé.

§ 2. La tranquillité

Une autre acception de la vie privée est la possibilité de ne pas être perturbé dans son quotidien. Il s'agit ici de la liberté de pouvoir s'isoler et de se prémunir contre les sollicitudes des tiers.

En somme, la tranquillité constitue le droit de contrôler l'accessibilité à soi. Le droit positif consacre ce droit et l'entoure de dispositions pénales strictes. Par exemple, le Code pénal sanctionne le harcèlement sexuel[59] ainsi que le harcèlement moral[60]. Notre système juridique reconnaît une sphère privée inviolable et qui exclue les tiers d'ingérences graves. Cela revient donc à dire que la vie privée est, à l'instar du droit de propriété, un droit exclusif.

[58] En français : Témoin de connexion.
[59] *C. pén.*, art. 222-33.
[60] *C. pén.*, art. 222-33-2 et 222-33-2-1.

§ 3. L'autonomie individuelle

La dernière dimension de la vie privée évoquée par Fabrice Rochelandet est plus difficile à cerner. L'autonomie individuelle renvoie à ce qui fait qu'un individu est unique, ce qui le rend particulier. Le secret n'est pas pertinent dans cette idée car ce qui singularise un individu peut et parfois doit être connu de tous. Dans cette idée, « *la vie privée peut ainsi se concevoir à travers l'affichage public, voire l'imposition aux autres, de son identité, de ses opinions et de sa manière de vivre* »[61].

Autrement dit, la vie privée renvoie également à une libre disposition de l'image renvoyée aux autres. C'est en somme « *l'aptitude à prendre des décisions importantes afin de développer une expression de soi et des relations intimes variées* »[62].

Loin d'être seulement théorique, cette dimension de la vie privée prend tout son sens à l'heure où l'image des individus déterminée sur la base d'algorithmes de plus en plus perfectionnés se substitue de plus en plus à leur image réelle. C'est d'ailleurs dans cette idée que s'inscrit l'article 10 de la loi informatique et libertés qui dispose qu' « *aucune décision de justice impliquant une appréciation sur le comportement d'une personne ne peut avoir pour fondement un traitement automatisé de données à caractère personnel destiné à évaluer certains aspects de sa personnalité* » et qu' « *aucune autre décision produisant des effets juridiques à l'égard d'une personne ne peut être prise sur le seul fondement d'un traitement automatisé de données destiné à définir le profil de l'intéressé ou à évaluer certains aspects de sa personnalité* ». Avec ce texte, les personnes sont protégées des décisions automatiques relatives à leur personnalité sans appréciation humaine. Malheureusement, la preuve d'un éventuel manquement à ce principe semble très difficile à rapporter dans la deuxième hypothèse.

Aussi, l'identité de l'individu trouve sa protection dans l'article 6 de la loi informatique et libertés qui dispose que les données personnelles « *sont adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs* ». Cet article est une garantie de l'intégrité de l'identité des personnes dans le monde numérique. Une telle garantie est d'autant plus importante que les données collectées, on peut le penser, n'approchent pas tout le temps la réalité de l'identité ou du comportement des personnes. En effet, le marketing ciblé trouve ses limites une fois que le

[61] Fabrice ROCHELANDET, *Economie des données personnelles*, La Découverte, 2010, p. 10
[62] *Ibid*.

consommateur a acheté le bien qu'il consultait en ligne mais qu'il reçoit encore de la publicité sur des produits identiques. Avec des phénomènes comme le Big Data, c'est-à-dire le traitement d'une masse gigantesque de données le plus rapidement possible, ces données sont vouées à être de plus en plus brutes et donc de moins en moins précises.

Après avoir exposé ces trois dimensions qui constituent la vie privée, il convient de présenter un panorama de la vie privée à l'ère du numérique.

Section 2. La vie privée à l'ère d'Internet

Le respect de la vie privée constitue un droit reconnu par les textes les plus fondamentaux de notre système juridique. Le Conseil Constitutionnel, dans plusieurs décisions, considère ce principe sur le fondement de l'article 2 de la DDHC de 1789[63]. La CESDHLF consacre également le droit au respect de la vie privée et familiale, de son domicile et de sa correspondance en son article 8. Le juge communautaire a, de surcroît, reconnu le droit au respect de la vie privées dès 1969[64] : ce droit est considéré comme un principe général du droit communautaire car il est fondé sur la tradition constitutionnelle commune aux Etats membres. En conséquence, le juge communautaire en assure le respect.

Il serait fastidieux d'étudier de manière plus approfondie la protection du droit au respect de la vie privée tant ce régime est vaste. Il est cependant certain que la notion est utile aux internautes dans la défense de leur droits malgré une certaine insécurité juridique (§2). Il conviendra avant toute chose de dresser un état des lieux de la vie privée sur Internet (§1).

§ 1. Etat des lieux de la vie privée sur Internet

Parfois, le débat sur le respect de la vie privée sur Internet laisse perplexe. Beaucoup de personnes ne se sentent pas concernées et répondent, après évocation des risques ou d'exemples d'atteintes, la phrase quasiment devenue sempiternelle : « *Je n'ai rien à cacher* ». L'emploi du pronom personnel de la première personne du singulier « *Je* » est très révélateur car sous-entend : « *Je ne me sens pas concerné tant que cela ne m'arrive pas personnellement* ». Dans un article intitulé « *La valeur sociale de la vie privée* » paru en 2009 sur le site Internet internetactu.net, Hubert Guillaud évoque le rapport de force déséquilibré entre les surveillants et les surveillés et de l'opacité généralisée de l'utilisation de données

[63] Par exemple, v. Cons. const., 23 juill. 1999, n° 99-416 DC, *Loi portant création d'une couverture maladie universelle*, cons. 45 ; Cons. Const., 10 mars 2011, n° 2011-626 DC, Loi d'orientation et de programmation pour le performance de la sécurité intérieure, cons. 69 etc.
[64] CJCE, 12 nov. 1969, aff. 29/69, *Erich Stauder c. Ville d'Ulm*.

personnelles dans le monde numérique, que ce soit sur leur collecte ou sur leur interprétation[65].

Pis, personne n'arrive à estimer la quantité et la qualité des données qu'il a pu, volontairement ou involontairement, laisser sur Internet. Cependant, une prise de conscience autour de ce problème commence à émerger, notamment avec le projet « *Design your privacy* »[66]qui propose des licences d'utilisation de données personnelles dans lesquelles la personne concernée choisit elle-même les conditions d'utilisation de ses données ainsi que les données en cause avec le responsable du traitement. Cette initiative innovante a le mérite de replacer le consentement effectif de la personne au premier plan, de manière bien plus forte que *l'opt-in*[67], et de rendre aux personnes un droit de propriété sur leurs données personnelles. Ce système avant-gardiste n'est pas utopique : il s'agirait *in fine* d'une gamme de licences que les « *entrepôts de données* » que sont les administrations, les associations et les entreprises pourront implémenter dans leurs systèmes[68].

En attendant, nous ne pouvons tous que constater que notre vie privée nous échappe de plus en plus (A) en raison de la diversité et de la multiplicité des moyens d'identifications (B).

A) Une vie privée fuyante

La notion d'identité est très difficile à appréhender dans le cyberespace. Les données personnelles ou traces numériques que nous laissons sur Internet sont multiples et diverses. Des tentatives de recensement de ces données ont été tentées, mais on ne peut admettre qu'elles balayent toutes les données possibles[69]. La loi et le règlement nous indiquent une liste non exhaustive de données d'identification mais dont l'objet est circonscrit par la répression des infractions[70].

Comme l'expose très bien le projet de Déclaration des Droits de l'Homme Numérique dans son exposé des motifs, « *sur Internet, chacun est identifiable ; ses affinités, ses amitiés, ses sentiments, ses goûts, ses modes de consommation, ses opinions, ses exigences morales,*

[65] Hubert GUILLAUD, « La valeur sociale de la vie privée », Internet Actu, 21 octobre 2009, [http://www.internetactu.net/2009/10/21/la-valeur-sociale-de-la-vie-privee/].
[66] En français : « Concevez votre vie privée ».
[67] En français : Le consentement préalable à un traitement de données.
[68] Thomas SAINT-AUBIN, « Design your privacy : pour une licence de partage des données personnelles », Internet Actu, 22 juin 2012, [http://www.internetactu.net/2012/06/22/design-your-privacy-pour-une-licence-de-partage-des-donnees-personnelles/].
[69] Fabrice ROCHELANDET, *Economie des données personnelles*, La Découverte, 2010, p. 15.
[70] *Décret relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne*, n°2011-219, 25 février 2011.

ses engagements politiques, syndicaux, ses convictions philosophiques, religieuses, peuvent parfaitement être enregistrés, classés, traités puis utilisés dans un but commercial, politique ou d'exclusion »[71].

Prenons l'exemple de l'anonymisation des décisions de justice. La CNIL considère que les bases de données jurisprudentielles sont des traitements automatisés de données au sens de l'article 5 de la loi informatique et libertés et doivent donc être déclarées auprès d'elle. Autrefois exclusivement utilisées par les juridictions et les professionnels du droit, ces bases de données se sont peu à peu ouvertes à Internet. De ce fait, des décisions de justices comportant le nom et l'adresse des parties furent bien plus largement diffusées qu'auparavant. Les décisions de justices peuvent comporter des données sensibles au sens de l'article 8, I de la loi du 6 janvier 1978 telles que les origines raciales, les opinions politiques, religieuses et syndicales, ou encore des données relatives à la vie sexuelle des personnes. En ce sens, la CNIL a recommandé en 2001 que « *l'occultation du nom des témoins et personnes physiques parties à l'instance devrait être appliquée, quelle que soit la nature de la décision, le fait même d'avoir été partie ou témoin lors d'un contentieux civil, pénal, prud'homal, administratif ou autre, constituant une information propice au préjugé et qui révèle, en tout cas, la situation de conflit que, par nature, la décision de justice aura tranchée.* »[72]

Le 12 juillet 2011, la formation contentieuse de la CNIL a sanctionné l'association *LEXEEK* qui publiait gratuitement sur Internet des décisions de justice non anonymisées. Des particuliers ayant découvert que certaines des décisions publiées les désignaient nommément, ils ont fait valoir leur droit d'opposition prévu à l'article 38 de la loi informatique et libertés. Devant le refus de l'association, ils ont déposé plainte auprès de la CNIL qui a condamné l'association *LEXEEK* à une amende de 10.000 euros et a enjoint *LEXEEK* de mettre fin à la mise en œuvre du traitement litigieux[73].

Donnant un effet effectif au droit à l'oubli, cette affaire révèle le type de données qui peuvent être publiées sur Internet. Cet exemple est en effet criant vu le nombre et la qualité des données d'identification qu'une décision de justice peut contenir. Cette affaire révèle

[71] Groupe de travail TIC, *Déclaration des droits de l'homme numérique*, Mairie d'Issy-les-Moulineaux, Livre blanc d'André SANTINI et d'Alain BENSOUSSAN, 20 novembre 2000, p. 10.
[72] CNIL, *Délibération portant recommandation sur la diffusion de données personnelles sur internet par les banques de données de jurisprudence*, n° 01-057, 29 novembre 2001, [http://www.cnil.fr/documentation/deliberations/deliberation/delib/17/].
[73] CNIL, *Délibération de la formation restreinte prononçant une sanction pécuniaire et une injonction de cessation de traitement à l'encontre de l'association LEXEEK*, n°2011-238, 30 août 2011, [http://www.cnil.fr/fileadmin/documents/La_CNIL/decisions/D2011-238_LEXEEK.pdf].

également les risques que peut entraîner ce type de traitement pour les personnes (en l'espèce, perte de chance d'obtenir un emploi par l'un des plaignants[74]).

Une simple page web, à but informatif cependant, est capable d'afficher des informations sur votre ordinateur[75]. La CNIL propose une petite expérience ludique sur son site Internet afin de sensibiliser les personnes sur leurs traces numériques et sur la facilité de leur ré-exploitation et de leur croisement[76]. Ces exemples sont très révélateurs de la manière dont nos données nous échappent d'une facilité déconcertante. Il est nécessaire de multiplier les exemples pédagogiques afin de sensibiliser les personnes sur leurs habitudes d'internautes. Ces données peuvent en effet être considérées comme des données permettant l'identification d'une personne au sens de l'article 2 de la loi informatique et libertés du 6 janvier 1978.

Même si ces données permettent au premier chef d'identifier un terminal informatique, les moteurs de recherche permettent déjà depuis plusieurs années de se créer un compte qui va assurer l'interconnexion entre un service de messagerie électronique, de navigation web (avec parfois stockage des mots clés), d'hébergement de contenu (image, texte ou vidéo), de consultation et de création de documents textes, de réseautage social, d'un service de *cloud computing*[77] … Ces informations concernent donc de moins en moins des terminaux informatiques mais de plus en plus des comptes d'utilisateurs souvent peu ou pas au fait de la politique de confidentialité du responsable du traitement et encore moins des finalités du traitement.

B) La diversité des moyens d'identification

Il est possible d'évoquer plusieurs éléments d'identification sur Internet. Il sera traité des principaux moyens d'identification. Bien sûr, les moyens qui seront évoqués resteront pertinents sous réserve des évolutions technologiques à venir !

Il sera donc traité des données liées au terminal de l'internaute (1), des témoins de connexion (2), de la mémoire cache (3) et enfin des données collectées par les moteurs de recherche et les réseaux sociaux (4).

---

[74] Anthony BEM, « Consécration des droits à l'oubli et à l'anonymisation des décisions de justice sur Internet », Legavox.fr, 12 oct. 2011, consulté le 12 mai 2013, [http://www.legavox.fr/blog/maitre-anthony-bem/consecration-droits-oubli-anonymisation-decisions-6655.htm].
[75] [http://www.anonymat.org/vostraces/index.php].
[76] [http://www.cnil.fr/vos-droits/vos-traces/].
[77] En français : « informatique dans les nuages ».

1) Les données liées au terminal de l'internaute

Dans cette catégorie, la principale donnée en cause est l'adresse IP qui est le moyen d'identifier de manière unique un terminal informatique connecté à Internet. L'IP peut être attribué de différentes façon, selon par exemple qu'elle soit attribuée par un FAI au terminal d'un particulier (dans la plupart des cas elle changera à chaque connexion, c'est l'IP « dynamique ») ou qu'elle soit attribué à un organisme plus important (elle sera fixe dans la plupart des cas). Cette donnée peut par exemple fournir des informations quant à la géolocalisation d'un individu. L'IP est à ce titre considérée comme une donnée à caractère personnel au niveau supranational[78] comme au niveau national[79].

D'autres données sont connues à chaque connexion sur un site : le système d'exploitation de l'ordinateur, le nom d'hôte ou les pages précédemment visitées.

2) Les témoins de connexion ou « *cookies* »

Ce sont de petits fichiers textes que le disque dur ou le navigateur employé de l'ordinateur enregistrent lors de chaque connexion à un site Internet. Le site qui les a créés pourra ainsi relire et reconnaître ces fichiers notamment dans le but de rendre les connexions ultérieures au même site plus rapides. Les cookies contiennent également un numéro unique qui sert à identifier le terminal. Ils peuvent donc être considérés, à l'instar de l'IP qui est aussi un identifiant unique, comme une donnée à caractère personnel au sens de l'article 4 de la loi informatique et libertés.

Les cookies permettent aux sites Internet de reconnaître un ordinateur. Ils sont par exemple employés à des fins de marketing comme la publicité ciblée. Pour la CNIL, le « *marketing ciblé* » est devenu le véritable « carburant » de l'économie numérique[80]. La collecte des cookies couplée avec celle des adresses IP est un réel enjeu économique car pour les commerçants, la publicité doit être ciblée au plus près de l'internaute pour générer plus de clics et ainsi être plus efficace[81]. Ce constat fait échos aux deux dimensions de la vie privée

[78] Groupe « Article 29 », *Avis sur le concept de données à caractère personnel*, 20 juin 2007.
[79] CNIL, « L'adresse IP est une donnée à caractère personnel pour l'ensemble des CNIL européennes », 2 août 2007, [http://www.cnil.fr/linstitution/actualite/article/article/ladresse-ip-est-une-donnee-a-caractere-personnel-pour-lensemble-des-cnil-europeennes/].
[80] CNIL, « Marketing ciblé sur internet : vos données ont de la valeur », 26 mars 2009, [http://www.cnil.fr/es/linstitution/actualite/article/article/marketing-cible-sur-internet-vos-donnees-ont-de-la-valeur/].
[81] Guillaume DESGENS-PASANAU, *La protection des données à caractère personnel, La loi informatique et libertés*, LexisNexis, 2012, p. 111.

qui ont été évoquées plus haut : le secret de la vie privée et la tranquillité sont largement atteintes par ce genre de pratiques.

Mais aussi intrusif soit-il, le marketing ciblé est le plan principal de l'économie numérique. Il n'est nullement question d'éradiquer toute publicité sur le web, aussi ciblée soit-elle. Mais l'économie des services numériques, bien que dynamique, ne doit pas se faire au détriment des droits des internautes. Un besoin de transparence émerge peu à peu : toute économie étant basée sur la confiance, les sites récoltant des informations dans un but marketing ont un intérêt indirect à recueillir le consentement préalable des utilisateurs/consommateurs.

3) La mémoire cache

La mémoire cache [82] est une mémoire qui stocke temporairement les pages précédemment visitées (ou d'autres données) dans le but de raccourcir le chemin parcouru par une requête en s'adressant directement et en premier lieu à cette mémoire, permettant ainsi une navigation plus rapide.

La mémoire cache présente certains risques car elle permet la duplication de données pour une durée parfois indéterminée. Par exemple, après l'exercice d'un droit d'opposition ayant conduit à l'effacement de données, les informations en cause peuvent survivre dans un répertoire cache.

4) Les données collectées par les moteurs de recherche et les réseaux sociaux

Du fait de leur utilisation massive et du nombre de données traité, les moteurs de recherche sont un foyer infini de données personnelles. Les algorithmes et les technologies de l'information se développant de surcroît à grande vitesse, les moteurs qui les utilisent réussissent néanmoins, grâce aux croisements de données, à se faire une idée de l'identité de chaque internaute.

Ces données peuvent être : des données de géolocalisation (grâce à l'adresse IP comme cela a été évoqué plus haut), des données relatives aux centres d'intérêts des personnes (grâce aux mots clés), les sites fréquentés par l'internaute… D'une manière générale, les moteurs de recherches sont les plus gros collecteurs de données non

[82] En français : « antémémoire ».

institutionnels. De plus, comme le souligne Guillaume Desgens-Pasanau, les moteurs de recherche sont tout à fait capables d'analyser des combinaisons de mots clés et d'en déduire un profil. L'exemple utilisé dans son ouvrage « *La protection des données à caractère personnel* » est le suivant : imaginons une requête composée des mots « synagogue Paris 11e arrondissement » combinée avec l'adresse IP de l'utilisateur. Le profil qui peut s'en déduire aura une valeur commerciale mais pourra, on peut l'imaginer, induire des risques en terme de vie privée, voire de libertés publiques[83].

Les réseaux sociaux quant à eux procèdent d'une façon un peu différente. Les données collectées reposent sur un consentement de l'utilisateur : ce dernier va remplir différents camps ou donner volontairement plusieurs informations à caractère personnel : nom et prénom, date de naissance, ville actuelle ou antérieure, professions, études, goûts artistiques, situation personnelle, orientation sexuelle, religion, opinions politiques, activités syndicales... Par exemple, Facebook permet l'extension de son réseau social par affinités ou par géolocalisation. L'utilisateur va ainsi pouvoir envoyer des demandes d'amitié à des personnes de la même ville ou université, à des personnes qui partagent les mêmes goûts artistiques[84] ou les mêmes aspirations professionnelles[85]. L'utilisateur, à chaque fois qu'il se connectera au réseau social depuis un nouveau terminal, enverra une nouvelle information géographique au prestataire de service. Enfin, l'utilisateur, lorsqu'il dépose une nouvelle photographie sur le serveur, aura la possibilité d'identifier d'autres utilisateurs et aussi de géolocaliser la photo. Ces exemples ne sont pas exhaustifs[86] mais permettent de comprendre la masse de données que peut traiter Facebook à partir d'un même compte.

La contrepartie du service délivré par Facebook sera une réexploitation des données par des services de régie publicitaire qui, à partir du profilage opéré, cibleront la publicité vers l'utilisateur. Facebook vend donc les données collectées à cette fin.

En résumé, les données collectées par ces deux types de services sont presque identiques bien que dans le cas des réseaux sociaux, la place du consentement est relativement mieux considérée. Cet éparpillement des données plus ou moins conscient doit nécessairement bénéficier d'un encadrement strict afin d'éviter des atteints aux droits et

[83] Guillaume DESGENS-PASANAU, *La protection des données à caractère personnel, La loi « informatique et libertés »*, LexisNexis, 2012, p. 106.
[84] Comme sur Myspace ou Youtube.
[85] Comme sur Viadéo ou LinkedIn.
[86] Il est en effet difficile d'anticiper toutes les possibilités. Facebook s'est implémenté avec de nombreux autres services qui peuvent être interconnectés avec le compte de l'utilisateur : contenus divers partagés, sites consultés…

libertés des personnes et au premier chef au droit au respect de la vie privée consacré à l'article 9 du Code Civil ainsi qu'à ceux garantis par la loi informatique et libertés du 6 janvier 1978.

§ 2. Les lacunes de la protection juridique de la vie privée sur Internet

Il est évident qu'aujourd'hui, les problématiques liées à la protection de la vie privée sur Internet doivent avant tout être appréhendées au niveau supranational. Pour preuve, beaucoup d'instances internationales « *classiques* » se positionnent sur cette question : Comité des ministres du Conseil de l'Europe, Commission européenne, Groupe « Article 29 », OCDE… Il est toutefois légitime de se poser la question de l'effectivité de cet encadrement institutionnel

En France, depuis la modification de la loi informatique et libertés en 2004, la CNIL a le pouvoir de sanctionner les responsables de traitements qui se trouvent en infraction avec cette loi. Ainsi, l'article 45, I de la loi informatique et liberté dispose :

« *I. - La formation restreinte de la Commission nationale de l'informatique et des libertés peut prononcer, après une procédure contradictoire, un avertissement à l'égard du responsable d'un traitement qui ne respecte pas les obligations découlant de la présente loi. Cet avertissement a le caractère d'une sanction.*

Le président de la commission peut également mettre en demeure ce responsable de faire cesser le manquement constaté dans un délai qu'il fixe. En cas d'urgence, ce délai peut être ramené à cinq jours.

Si le responsable du traitement se conforme à la mise en demeure qui lui est adressée, le président de la commission prononce la clôture de la procédure.

Dans le cas contraire, la formation restreinte peut prononcer à son encontre, après une procédure contradictoire, les sanctions suivantes :

1° Une sanction pécuniaire, dans les conditions prévues par l'article 47, à l'exception des cas où le traitement est mis en œuvre par l'Etat ;

2° Une injonction de cesser le traitement, lorsque celui-ci relève des dispositions de l'article 22, ou un retrait de l'autorisation accordée en application de l'article 25. »

Mais le juge judiciaire fait concurrence à la CNIL en ce qu'il est compétent dans le contentieux de la réparation des dommages occasionnées lors d'un traitement de données. Dans une ordonnance de référé du 14 avril 2008, le TGI de Paris s'est déclaré compétent pour

statuer sur la demande en réparation d'un requérant sur le fondement de la loi informatique et liberté[87].

Dans cette affaire, le TGI de Paris a mis la société Google hors de cause car l'article 5 de la loi informatique et libertés qui dispose que les traitement qui sont soumis à cette loi les traitement « *Dont le responsable, sans être établi sur le territoire français ou sur celui d'un autre Etat membre de la Communauté européenne, recourt à des moyens de traitement situés sur le territoire français* » ne pouvait pas permettre d'engager la responsabilité de Google en l'espèce car les moyens de traitement (les serveurs) étaient basés aux Etats-Unis.

Dans une autre affaire datant de 2006, le TGI de paris a reconnu la responsabilité de Google cette fois ci sur le fondement de l'article 9 du Code civil qui consacre le droit au respect de la vie privée et sur celui de la LCEN[88].

De ces décisions ressort le constat d'une insécurité juridique qui joue au détriment des internautes. En effet, nombreux traitements (navigateurs web, moteurs de recherche, réseaux sociaux) ayant leurs moyens de traitement aux Etats-Unis, les droits reconnus par la loi informatique et liberté ne sont pas effectifs dans ces cas là.

Pourtant, il apparaît plus que jamais nécessaire d'assurer le respect de ces droits à l'heure d'Internet et des traitements de plus en plus perfectionnés.

[87] TGI de Paris, ord. de référé, 14 avril 2008, *Bénédicte S / Google Inc., Google France.*
[88] TGI de Paris, ord. deréféré, 19 octobre 2006, *Mme H.P. c/ Google France.*

Chapitre 3. Les contours du droit à l'anonymat

L'anonymat sur Internet n'est pas chose facile à délimiter. D'une part parce que l'anonymat total devient impossible de fait. Nous sommes en effet devenus de petites mines de données tout en exerçant notre liberté de communication en ligne. Cependant, nous essaierons de dégager deux dimensions essentielles de l'anonymat (Section 1) avant de se tenter à rassembler en un corpus des règles qui tendent à protéger les différentes dimensions que l'anonymat implique (Section 2).

Section 1. L'anonymat : un concept à deux dimensions

Il est en effet assez difficile de cerner les contours exacts de l'anonymat. Si on prend l'anonymat comme un droit à ne pas être reconnu, les raisons de l'exercice d'un tel droit peuvent être fondées tant sur la volonté de prévenir les atteintes à sa vie privée (§1) que sur celle d'assurer l'intégrité de son identité (§2).

§1. L'anonymat comme droit préventif des atteintes à la vie privée

Du point de vue de la technique informatique, l'anonymat pose trop de contraintes pour un utilisateur moyen. Personne n'est réellement anonyme sur Internet. De plus, un anonymat total ne serait pas tolérable car il aurait pour effet de placer les personnes en situation d'impunité vis-à-vis des garants de l'ordre public et des tiers qui auraient à se plaindre d'atteintes légitimes à leurs droits et liberté. Aussi, un anonymat total ne serait pas opportun pour le développement des relations numériques : les utilisateurs désirent être reconnus par leur boutique en ligne préférée, ne serait-ce que pour bénéficier de points de fidélité ou de réduction. Des techniques d'anonymisation ne seraient de surcroît pas populaires car peut-être trop complexes d'utilisation et pas forcément accessibles d'un point de vue financier. Cependant, de telles techniques doivent rester possibles sur le fondement de l'article 30 de la LCEN qui dispose que « *l'utilisation des moyens de cryptologie est libre* ».

Mais si un anonymat total est impossible, un droit à l'anonymat circonscrit est envisageable. A l'instar du régime institué par le législateur de 2004 pour les éditeurs à titre non professionnel, un droit à l'anonymat préventif des atteintes à la vie privée est possible alors que dans la protection de la vie privée, le rôle du juge judiciaire, en vertu de l'article 9 du Code civil, est un rôle de réparation des dommages constatés. La même réflexion peut s'appliquer dans le paradigme énoncé à l'article 1 de la loi informatique et libertés qui dispose

que « *L'informatique doit être au service de chaque citoyen* » et qu'elle ne doit porter atteinte, entre autres, à l'identité humaine.

Mais ce droit ainsi énoncé et garanti par le Code Civil ne pourrait-il pas attester l'existence d'un droit préventif des atteintes à la vie privée ? De même que cette garantie peut justifier l'existence du régime des éditeurs de contenu à titre non professionnel qui est un régime préventif des atteintes à la liberté d'opinion et d'expression et au droit au respect de la vie privée de manière incidente. L'exigence d'une telle prévention des risques repose sur des considérations philosophiques. C'est l'autonomie individuelle qui apparaît ici être le fondement le plus intéressant. D'autres auteurs préfèrent parler d'autonomie « *informationnelle* »[89] à l'instar du Tribunal fédéral allemand[90] qui se fondait sur le droit au libre développement de soi reconnu par la loi fondamentale allemande. La juridiction suprême allemande a en effet considéré que ce droit à l'autodétermination informationnelle « *comprend l'autorité de l'individu de décider pour lui-même – sur la base du concept d'autodétermination – quand et dans quelles mesures des faits relevant de sa vie privée pourront être révélés à autrui* ». Cette « *autorité* » de l'individu n'est pas considérée comme un droit de propriété, exclusif par nature, mais comme un moyen de prévention contre les situations qui limitent « *la liberté de l'individu de planifier ou de décider sans être soumis à des pressions ou influences* […]. *Le droit à l'autodétermination en matière d'information exclut un ordre social ou légal dans lequel les citoyens ne pourraient plus savoir qui sait quoi sur eux, quand et à quelles occasions.* »

En somme, les véritables problèmes ne sont pas tant les traitements de données personnelles en eux-mêmes mais le déficit d'information des individus quant à l'utilisation réelle de ces données et quant aux risques d'exposition involontaires.

Suivant cette conception très avant-gardiste du Tribunal fédéral allemand, le droit au respect de la vie privée engloberait donc un ensemble de règles effectives et préventives des atteintes à la vie privée. Il s'agirait donc de redonner à l'individu la place qui lui revient, naturellement aurait-on envie de dire, dans les traitements qui sont opérés sur ses données personnelles.

Quoi qu'il en soit, le droit à l'anonymat peut légitimement être considéré comme un ensemble de règles préventives dès le moment où l'on admet que ce droit n'est pas un droit à

[89] Daniel KAPLAN, *Informatique, libertés, identités*, Editions FYP, 2010, p. 69.
[90] Tribunal fédéral allemand, 15 déc. 1983, *Volksählungsgesetz*, BverfGE 65, 1, 41.

la non-identification totale. Il est aujourd'hui inconcevable d'entraver totalement l'identification des individus, mais le fait d'encadrer au mieux les données identificatrices afin qu'elles ne se retournent pas contre les personnes qu'elles concernent correspond aux principes de l'anonymat, à savoir respecter le choix des personnes à préserver leur identité de toute dénaturation et assurer le respect de leur vie privée. C'est là le véritable sens de l'anonymat numérique.

§2. L'anonymat comme droit au respect de l'identité

L'anonymat peut parfois ne pas recouvrir la vie privée. La Chambre Criminelle a, par exemple, pu reconnaître que la demande d'écoute faite par un agent de police servait à percer l'anonymat d'un suspect sans pour autant porter atteinte à sa vie privée car les conversations n'étaient pas enregistrées[91].

Il est possible de trouver dans la loi quelques indices laissant penser que vie privée et identité ne se confondent pas toujours. L'article 1 de la loi informatique et libertés de 1978 fait également une distinction entre la vie privée et « *l'identité humaine* ». La tendance à confondre anonymat et vie privée réside dans de fait que les deux notions sont parfois touchées simultanément.

Enfin, dans le Code Pénal, les infractions portant atteinte à la vie privée et les atteintes aux personnes résultant des fichiers ou des traitements informatiques font l'objet d'une section distincte au sein du chapitre relatif aux atteintes aux personnes.

Il s'agit là cependant d'un postulat théorique. A l'heure d'Internet, les données en apparence seulement identifiantes permettent le plus souvent de porter atteinte à la vie privée. C'est par exemple le cas des « *tags* » sur les photos déposées sur Facebook. Les noms et prénoms d'une personne peuvent être associés à une photos dont le degré d'intimité peut être plus ou moins élevé. Ainsi, c'est pourquoi les atteintes à l'anonymat pourront tantôt porter atteinte à la vie privée, tantôt à l'identité.

Aussi, la question de l'hétéronymat, ce droit aux identités multiples, mérite également d'être posée. En apparence, ce droit semble permettre une impunité a l'instar d'un droit à l'anonymat total. Mais nous verrons que les pistes à l'étude sont toutes autres.

[91] Crim., 4 et 16 janvier 1974, JCP 1974, II 17731.

Section 2. Quel corpus de règles pour le droit à l'anonymat ?

Ce corpus du droit à l'anonymat est encore en gestation et sera ici considéré comme l'ensemble des règles préventives des atteintes à la vie privée et à l'identité. Il sera successivement traité des droit des personnes fichées (§1) puis de obligations préventives imposables aux responsables de traitements (§2).

Même si le projet de règlement européen général sur la protection des données personnelles sera la principale source d'analyse des possibilités envisageables, d'autres pistes juridiques ou extra-juridiques seront évoquées.

§1. Les droits des personnes fichées

Il sera successivement traité des exigences relatives à l'intégrité de l'identité des personnes (A), de celles relatives à leur consentement et à leur information (B). Il sera également soulevé la question de la portabilité des données (C) avant de terminer par une brève réflexion sur l'hétéronymat (D).

A) Le renforcement du contrôle de l'adéquation, de l'exactitude et de la proportionnalité des données par rapport aux finalités du traitement

C'est l'article 6- 3° de la loi informatique et liberté qui pose le principe selon lequel les données personnelles collectées sont adéquates, exactes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitement ultérieurs.

Elles sont bien évidemment collectées de manière loyale et licite pour des finalités « *déterminées, explicites et légitimes et ne sont pas traitées ultérieurement de manière incompatible avec ces finalités* ».

C'est l'article 5 du projet de règlement général sur la protection des données qui encadre ces exigences. Des nouvelles notions sont rajoutées. Ainsi, l'article 5- a) énonce que les données sont traitées de manières loyale, licite et transparente au regard de la personne concernée. L'obligation de transparence induirait donc une présentation claire, lisible et complète (par exemple, on peut l'imaginer, au moyen d'une infographie).

Le c) du même article reprend les exigences classiques de l'adéquation, l'exactitude et la proportionnalité des données par rapports aux finalités du traitement tout en rajoutant un principe de minimisation de la collecte des données. Partant, il s'agit de contraindre le

responsable du traitement de demander seulement les données strictement nécessaires pour remplir les finalités du traitement.

Selon Maître Alain Bensoussan, le principe de minimalisation des données contraindra le responsable du traitement à se justifier du caractère nominatif des données collectées[92]. Ainsi, l'anonymat deviendrait un principe et l'identification l'exception.

Ces règles sont donc avant tout protectrices de l'intégrité de l'identité des personnes. Mais les règles préventives des atteintes à la vie privée sont elles aussi amenées à être renforcées.

B) Vers une meilleure reconnaissance du consentement et du droit à l'information préalable des personnes

L'article 7 de la loi informatique et libertés dispose qu'un traitement est légitime dès lors que le consentement de la personne a été recueilli, tout en prévoyant des cas où ce consentement n'est pas nécessaire (obligation légale incombant au responsable du traitement, sauvegarde de la vie de la personne concernée, exécution d'une mission de service public etc.). L'exception prévue au 5° de cet article est cependant très large et permet d'éluder le principe du consentement préalable dans beaucoup de cas. Cette exception peut être mise en œuvre dans le cas où « *La réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le destinataire, sous réserve de ne pas méconnaître l'intérêt ou les droits et libertés fondamentaux de la personne concernée* », est avancée par le responsable du traitement. L'article 32-II prévoit également un consentement préalable concernant l'implémentation des témoins de connexion.

L'article 2 de la directive 95/46/CE dispose, quant à elle, que le consentement doit être libre, spécifique et informé (il peut donc s'agir d'une page à cocher ou d'une mention spécifique, mais jamais d'un consentement implicite).

Le futur règlement général sur la protection des données adopte une nouvelle position sur ce sujet. D'abord, le responsable du traitement aura la charge de la preuve du consentement préalablement donné par la personne fichée. Cette dernière aura le droit de retirer son consentement à tout moment sans que cela remette en cause la licéité du traitement

[92] Conférence de Maître Alain Bensoussan sur le droit du Big Data à l'Université Supinfo, 2 avr. 2013, disponible en vidéo sur [http://www.youtube.com/watch?v=GMaDBckRtMc].

auquel elle avait préalablement donné son consentement. C'est donc un rétablissement de l'ordre logique entre « *l'opt in* » et « *l'opt out* ».

Enfin, et c'est le point le plus original et le plus intriguant, le consentement ne constituera pas « *un fondement juridique valable pour le traitement lorsqu'il existe un déséquilibre significatif entre la personne concernée et le responsable du traitement* ». La notion de « *déséquilibre significatif* » sera soumise à la libre appréciation des juges nationaux. Dans le cas d'une reconnaissance d'un « *déséquilibre significatif* », qui sera interprété à la lumière des conditions générales d'utilisation ou bien sans doute des « *privacy policies* »[93], le responsable du traitement ne pourra valablement se fonder sur le consentement de l'utilisateur. En somme, cela revient à dire qu'en cas de déséquilibre significatif constaté le traitement sera illicite au regard de l'article 6- a) du règlement qui dispose qu'un traitement est licite notamment si « *la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques* ».

On peut espérer que tel sera le cas. Toujours selon l'article 6, le responsable du traitement pourra toujours justifier d'un intérêt légitime qu'il poursuit pour écarter la nécessité du consentement préalable « *à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée, qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant*. » Une telle règle sera bien évidemment laissée à l'appréciation souveraine des juges mais on peut espérer qu'ils seront incités à être plus attentifs aux droits et libertés qui peuvent être mis en causes dans le cadre d'un traitement de données personnelles.

Bien que cette règle ne soit pas véritablement préventive, elle fait peser sur les responsables de traitements une lourde responsabilité ayant un effet préventif en ce qu'ils devront, afin d'éviter toute sanction, des attitudes diligentes.

L'aspect préventif de la future réforme se retrouve aussi avec le renforcement de l'obligation d'information préalable. L'article 32 de la loi informatique et libertés prévoit les informations qui doivent préalablement être fournies à la personne auprès de laquelle les données à caractère personnel vont être recueillies. Ces informations concernent notamment la finalité du traitement, les destinataires ou catégories de destinataires des données, les droits dont elle dispose en vertu de la loi informatique et libertés et de la possibilité d'un transfert des données vers des Etats hors UE.

[93] En français : « politiques relatives à la vie privée ».

L'article 14 de la proposition de règlement général sur la protection des données personnelles impose de nouvelles informations obligatoirement communiquées. Il s'agit par exemple de l'identité du responsable du traitement, ses coordonnées, la durée pendant laquelle les données seront conservées, l'existence des droits invocables par la personne au titre du règlement, le droit d'introduire une réclamation auprès de l'autorité de contrôle et les coordonnées de cette autorité, la possibilité d'un transfert de données vers un Etat tiers à l'UE par référence à une décision relative au caractère adéquat du niveau de protection rendue par la Commission ainsi que « *toute autre information nécessaire pour assurer un traitement loyal des données à l'égard de la personne concernée, compte tenu des circonstances particulières dans lesquelles les données à caractère personnel sont collectées* ».

Ces informations sont obligatoirement communicables sous réserve des exceptions prévues au même article. La Commission aura en outre le pouvoir d'établir des formulaires types pour la communication des informations prévues en vertu de l'article 14 « *compte tenu des caractéristiques et des besoins particuliers des différents secteurs et, le cas échéant, des situations impliquant le traitement de données* ». On peut donc imaginer une standardisation des informations transmises dans les secteurs du commerce électronique et des réseaux sociaux mais aussi dans le secteur public et parapublic, même si ces deux secteurs sont souvent couverts par les exceptions imposées par la loi relatives à des missions de service public ou de sauvegarde de la vie des personnes.

Enfin, la proposition de règlement en son article 31 va généraliser à l'ensemble des responsables de traitements l'obligation de notifier aux personnes les failles de sécurité.

Cet ensemble de règles relatives au consentement et à l'information des personnes auraient un réel effet préventif qui va dans le sens d'un droit à l'anonymat concernant les traitements de données s'effectuant sur Internet. On peut en imaginer les effets bénéfiques notamment sur l'utilisation des réseaux sociaux.

C) La portabilité des données : vers une gestion proactive des données personnelles

Faire pleinement participer l'individu dans la gestion de ses données est une approche intéressante et très novatrice. Il ne s'agit pas ici d'imaginer un droit de propriété des personnes sur leur données car l'effet serait semble-t-il dommageable pour le développement des relations numériques.

La portabilité des données permettrait aux personnes d'adopter une position proactive et non plus passive dans le processus de collecte des données. Il s'agirait en fait de permettre aux internautes de « porter » et de partager ses données entre plusieurs systèmes et services tout en surveillant de manière rapprochée le contrôle sur les données en causes.

Paradoxalement, cette idée n'est pas forcément contraire au respect de la vie privée. Si l'utilisateur possède un réel contrôle sur son identité numérique, il peut ainsi lutter contre l'éparpillement de ses données et en contrôler l'exactitude. Il peut aussi disposer de plusieurs identités dont il assure lui-même la gestion.

C'est l'article 18 de la proposition de règlement qui va peut-être ouvrir cette possibilité révolutionnaire. En effet, le 2 de cet article dispose que « *Lorsque la personne concernée a fourni les données à caractère personnel et que le traitement est fondé sur le consentement ou sur un contrat, elle a le droit de transmettre ces données à caractère personnel et toutes autres informations qu'elle a fournies et qui sont conservées par un système de traitement automatisé à un autre système dans un format électronique qui est couramment utilisé, sans que le responsable du traitement auquel les données à caractère personnel sont retirées n'y fasse obstacle*. »

On peut espérer plusieurs effets bénéfiques. Des services de gestion des données personnelles pourront par exemple être lancés. La question des formats des données se posera cependant, mais l'utilisation d'un format libre est envisageable. Aussi, la portabilité des données ainsi envisagée permettrait un exercice plus effectif des droits reconnus aux individus, notamment du droit d'accès et de rectification.

D'autres possibilités sont aussi en gestation. Par exemple, le « *vendor relationship management* »[94] est une idée qui mérite d'être approfondie. Cette notion peut être considérée comme une forme plus aboutie de la portabilité des données car elle permet de rééquilibrer les relations entre vendeurs et consommateurs en rendant ces derniers moins captifs. Les clients seraient en fait le point d'intégration de leurs données, contrôleraient les données qu'ils produisent et réunissent et choisiraient avec qui, quand et dans quels termes ils partageraient ces données. Les clients définiraient eux-mêmes les conditions d'utilisation de leurs données et seraient libres d'exprimer leurs demandes et intentions en dehors du contrôle d'un tiers. Le projet « *Design your privacy* » est une expression française de ce concept. Des modèles de licences d'exploitation de données personnelles ont été élaborés afin d'accompagner

[94] En français : « gestion de la relation fournisseur ».

l'internaute consommateur. A noter qu'une de ces licences prévoit une concession d'exploitation de données anonymisées[95]. Un droit à l'anonymat contractuel est donc envisageable !

On pourrait reprocher à ce concept d'être peut-être trop complexe pour l'internaute moyen qui demande une simplification de plus en plus poussée, surtout lorsqu'il est internaute consommateur. Aussi, aucune garantie de fonctionnement n'est assurée : les vendeurs ne sont pas encore prêts à dialoguer avec des entrepôts de données.

D) Le droit à l'hétéronymat en question

Daniel Kaplan a une vision originale de l'hétéronymat. Dans son ouvrage « Informatique, libertés, identités », il estime que « *Favoriser le développement de l'hétéronymat, le jeu organisé de construction et de valorisation de personnalités plus ou moins cloisonnées, aurait du sens aujourd'hui, tant pour protéger l'individu actif sur les réseaux contre d'éventuelles « fuites » reliant à son insu ses différents univers de vie, que pour lui permettre d'explorer et de développer les différentes facettes de sa personnalité. Il faudra des outils et peut-être du droit* »[96].

Le rapport de sénateurs Yves Détraigne et Anne-Marie Escoffier « La vie privée à l'heure des mémoires numériques » se prononçait également en faveur de la reconnaissance d'un droit à l'hétéronymat et ont même tracé les grandes d'un régime légal de ce droit : « *Chaque individu pourrait se forger de véritables personnalités alternatives, distinctes de la personnalité civile qui les exploite. Afin d'éviter que ce droit ne serve à commettre des infractions, ces identités alternatives pourraient être déposées auprès d'un organisme chargé de les gérer. En cas d'infractions par exemple, la justice pourrait demander l'identité civile de la personne* »[97].

L'idée d'une reconnaissance légale d'identité alternative est restée en suspend jusqu'à ce jour. Certains auteurs s'opposent à la reconnaissance d'un tel droit et lui préfèrent un droit

---

[95] [http://www.patrimoine-immateriel.fr/licences-partage-donnees-personnelles/licence-design-your-privacy-de-stock-comprenant-des-donnees-personnelles-anonymisees-dyp-sa/].

[96] Daniel KAPLAN, *Informatique, libertés, identités*, Editions Fyp, 2010, p. 112.

[97] Yves DETRAIGNE, Anne-Marie ESCOFFIER, *La vie privée à l'heure des mémoires numériques. Pour une confiance renforcée entre citoyens et société de l'information*, Rapport d'information n°441 (2008-2009), 27 mai 2009, p. 107, [http://www.senat.fr/rap/r08-441/r08-4411.pdf].

à l'anonymat total[98], ce qui est peu souhaitable sans plus de précisions quant à son encadrement.

§2. Les obligations des responsables de traitements

On peut envisager plusieurs sortes de moyens juridiques pour contraindre les acteurs du web d'améliorer la protection de l'anonymat dans ses deux dimensions fondamentales. Le renforcement de la transparence est, sans aucun, doute une exigence nécessaire (A). Il conviendra aussi d'explorer la piste du concept de « *privacy by design* » (B) et de l'engagement responsable (C). Pour finir, nous évoquerons les enjeux que représente la labellisation (D).

A) Le renforcement de la transparence

Dans le régime de la loi informatique et libertés de 1978, l'article 6 dispose que les données doivent être collectées de manière loyale, licite, pour des finalités déterminées, explicites et légitimes. Aussi, elles ne doivent pas être traitées ultérieurement de manière incompatible avec ces finalités. Enfin, elles doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs.

Ces exigences législatives strictes permettent d'encadrer la demande de données à caractère personnel en vertu du critère de la finalité du traitement. Cela suppose donc que la finalité du traitement soit donc connue par l'internaute. C'est, par exemple, le cas pour certains sites de vente en ligne lorsqu'ils proposent, après la collecte de l'adresse mail du consommateur, l'envoi d'annonces publicitaire sur la boîte mail communiquée.

Cependant, cette information est beaucoup plus opaque concernant les moteurs de recherche et les sites de réseaux sociaux. L'accès aux informations relatives à la finalité du traitement est souvent déconcertante et peu lisible pour des non juristes et a fortiori pour des jeunes et vieilles personnes. L'internaute averti et responsable n'est pas la norme sur Internet mais bien l'exception. C'est pourquoi un renforcement de la transparence est souhaitable.

La proposition de règlement « *relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données*[99] »

[98] Olivier ITEANU, « Droit à l'oubli numérique, hétéronymat et cassoulet », Iteanu Blog, 19 fév. 2010, [http://blog.iteanu.com/index.php?post/2010/02/19/34-droit-a-loubli-numerique-heteronymat-et-cassoulet].

consacre ainsi deux nouveaux critères qui viennent s'ajouter à ceux initialement prévus à l'article 6 de la directive 95/46/CE dont les termes ont été repris par l'article 6 de la loi informatique et libertés. Il s'agit du principe de collecte transparente et du principe de minimisation des données demandées.

Classiquement, l'exercice du droit d'information s'effectue a posteriori du traitement, dans la possible hypothèse d'exercer son droit à l'oubli. Ici, le droit à l'information se voit conférer un caractère préventif. De manière volontairement incidente, il s'agit ici de favoriser les conditions de l'expression d'un consentement libre, éclairé et circonstancié.

Cette transparence de l'information devrait permettre à l'utilisateur de connaître les finalités réelles du traitement, la durée de conservation des données, leur possible transfert, les destinataires de l'information de manière plus effective. C'est donc la maîtrise que l'internaute a sur ses données qui est renforcée, ce qui va dans le sens d'un droit à l'anonymat.

B) Le respect de la vie privée dès la conception ou « *privacy by design* »

Derrière cette expression anglaise qui pourrait se traduire par « *respect de la vie privée dès la conception* » se cache un concept très prometteur qui s'inscrit dans la philosophie de l'adage « *code is law* »[100] théorisé il y a maintenant 13 ans par le professeur et juriste américain Lawrence Lessig[101]. Il s'agit de faire prendre en compte par défaut aux machines les règles relatives à la protection de la vie privée. De manière originale, il s'agit de légiférer dans les codes sources des logiciels ou dans les algorithmes. Cette idée est notamment issue de l'impulsion du Groupe international de travail sur la protection des données dans les télécommunications[102].

Bien que ce principe soit absent de la loi française et de la directive 95/46/CE, la proposition de règlement général sur la protection des données prévoit en son article 23- 1 que « *Compte étant tenu des techniques les plus récentes et des coûts liés à leur mise en œuvre, le responsable du traitement applique, tant lors de la définition des moyens de traitement que lors du traitement proprement dit, les mesures et procédures techniques et organisationnelles*

---

[99] *Proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données)*, 2012/0011 (COD), 25 jan. 2012, art. 5.
[100] En français : « le code (au sens informatique du terme) est la loi ».
[101] Lawrence LESSIG, « Code is law, On liberty in cyberspace », Harvard magazine, jan.-fév. 2000, [http://harvardmagazine.com/2000/01/code-is-law-html]. Pour une traduction française de l'article : [http://www.framablog.org/index.php/post/2010/05/22/code-is-law-lessig].
[102] Groupe international de travail sur la protection des données dans les télécommunications, *Privacy by Design and Smart Metering : Minimize Personal Information to Maintain Privacy*, 675.43.18, 12-13 sept. 2011.

appropriées de manière à ce que le traitement soit conforme aux prescriptions du présent règlement et garantisse la protection des droits de la personne concernée. »

Et afin de renforcer ce principe, le 2 du même article dispose que « *Le responsable du traitement met en œuvre des mécanismes visant à garantir que, par défaut, seules seront traitées les données à caractère personnel nécessaires à chaque finalité spécifique du traitement, ces données n'étant, en particulier, pas collectées ou conservées au-delà du minimum nécessaire à ces finalités, pour ce qui est tant de la quantité de données que de la durée de leur conservation. En particulier, ces mécanismes garantissent que, par défaut, les données à caractère personnel ne sont pas rendues accessibles à un nombre indéterminé de personnes physiques*. »

Cette disposition s'avère particulièrement intéressante si on la conçoit à travers le prisme des réseaux sociaux et des moteurs de recherche. Par exemple, lors de la création d'un compte Facebook, le profil est actuellement public par défaut : lors d'une simple recherche sur un navigateur web, le compte Facebook du nouvel utilisateur sera consultable par l'auteur de la requête sans qu'il fasse parti de son cercle d'amitié. On peut imaginer le genre de dérive qu'un tel réglage par défaut peut engendrer : l'exemple de l'employeur qui fait une « recherche Google » sur son candidat est toujours parlant mais on peut aussi évoquer la facilité que cela engendre pour les pratiques d'escroqueries ou encore pour les délinquants pédophiles.

A propos des paramétrages par défaut des navigateurs web, si les textes précédemment cités permettront par exemple une gestion plus respectueuse de la vie privée par exemple en activant par défaut la fonction « *ne pas pister* » qui indique aux sites web de renoncer au pistage par les annonceurs et autres parties tierces de l'internaute ou en activant par défaut l'effacement de l'historique (actuellement conservé par défaut par les navigateurs web).

A noter que ces mesures, si elles sont adoptées en l'état, s'accompagneront d'initiatives complémentaires qui ont déjà cours aujourd'hui. Les « *privacy enhancing technologies* »[103] s'inscrivent en effet dans la même logique. Par exemple, le système P3P « *permet un dialogue automatique et immédiat, par agents logiciels interposés, entre la*

[103] En français : « technologies protectrices de la vie privée ».

politique de confidentialité de ses données, préconfigurée par l'utilisateur et l'usage que le responsable a l'intention d'en faire »[104].

Ainsi les internautes auront le choix entre une visibilité plus forte si, par exemple, ils souhaitent améliorer les services qu'ils utilisent et une navigation anonymisante et plus protectrice de la vie privée qui serait donc prévue par défaut. Par ailleurs, certaines personnalités du milieu informatique réfléchissent à des technologies permettant de personnaliser sans identifier en se posant la question simple : « *Ai-je besoin de tout connaître pour vous reconnaître ?* ». Les pistes données par l'informaticien californien Alfred Kobsa ont pour objectif une personnalisation des services qui va de paire avec la protection des données[105]. Ces pistes traitent à ce titre de la rationalisation des données demandées à l'utilisateur.

C) L'engagement responsable ou « *accountability* »

C'est un concept aussi connu sous le nom d' « *accountability* ». En pratique, l'*accountability* renvoie à « *l'ensemble des mesures internes prises par un responsable de traitement afin d'attester de son niveau de conformité à la règlementation applicable*[106] ». Ces mesures internes peuvent par exemple concerner « *la mise en place d'une procédure de gestion des plaintes, la réalisation d'audits internes ou externes, la réalisation de privacy impact assessments, la désignation d'un correspondant informatique et liberté ou encore l'adoption de binding corporate rules visant à encadrer les transferts de données en dehors de l'Espace économique européen* »[107].

La proposition de règlement européen a pris en compte ce nouveau concept à travers plusieurs articles. L'article 5- f) impose par exemple que le responsable du traitement rapporte la preuve de son respect de l'ensemble des dispositions du règlement.

L'article 11 impose au responsable du traitement d'appliquer « *des règles internes transparentes et facilement accessibles en ce qui concerne le traitement des données à caractère personnel et en vue de l'exercice de leurs droits par les personnes concernées* » dans le but d'obliger à la vulgarisation des conditions d'exercice des droits des utilisateurs.

---

[104] Ludovic PAILLER, *Les réseaux sociaux sur internet et le droit au respect de la vie privée*, Larcier, 2012, p. 179.
[105] Alfred KOBSA, « Privacy-Enhanced Personalization », Communications of the ACM, 2007, [http://www.ics.uci.edu/~kobsa/papers/2006-CHI-kobsa.pdf].
[106] Guillaume DESGENS-PASANAU, *La protection des données à caractère personnel, La loi « informatique et libertés »*, LexisNexis, 2012, p. 182.
[107] *Ibid*.

L'article 12 vient, quant à lui, encadrer les procédures permettant l'exercice des droits à l'information, d'accès et de rectification.

L'article 22 instaure une obligation d'établir des règles internes et de définir des mesures appropriées afin de garantir et démontrer le respect du règlement, notamment sur le recensement des traitements, l'obligation de sécurité, l'accomplissement des formalités préalables et la désignation d'un correspondant à la protection des données. Le 3 du même article prévoit également l'obligation de diligenter des audits internes ou externes sur le respect des obligations énoncées. Gageons que le marché de l'audit va encore se développer dans ce secteur.

Enfin, des études d'impact sont imposées aux articles 33 et 44 à propos des traitements comportant des risques particuliers ou sur la mise en œuvre de certaines exceptions à l'encadrement d'un transfert de données en dehors de l'UE.

D) La labellisation

L'article 11- 3°- c) de la loi informatique et libertés dispose que la CNIL « *délivre un label à des produits ou à des procédures tendant à la protection des personnes à l'égard du traitement des données à caractère personnel, après qu'elle les a reconnus conformes aux dispositions de la présente loi dans le cadre de l'instruction préalable à la délivrance du label par la commission.* »

Pour Guillaume Desgens-Pasanau, ce pouvoir de labellisation permet à la CNIL d'adopter une véritable politique en faveur d'outils ou procédures respectueuses des principes posés par la loi dont elle est la gardienne et lui confère, en outre, un réel pouvoir de communication[108]. Cette capacité lui permettrait également de « *renforcer son statut de régulateur économique pouvant orienter le marché vers les solutions les plus protectrices en matière de vie privée* »[109].

La labellisation permettrait progressivement d'établir des référentiels en matière de protection des données. A noter que le projet de règlement s'inscrit également dans cette démarche. En effet, l'article 39 prévoit le principe d'un mécanisme de certification placé sous le contrôle de la Commission. Il est souhaitable que de tels mécanismes ne restent pas lettre

[108] Guillaume DESGENS-PASANAU, *La protection des données à caractère personnel, La loi « informatique et libertés »*, LexisNexis, 2012, p. 184.
[109] *Ibid*.

morte car ils constituent un réel enjeu de communication sur la protection des données. Malheureusement, à ce jour, la CNIL n'a encore labellisé aucun traitement.

L’anonymat est donc une notion aux contours incertains mais qui touche des sujets sociétaux d’une importance capitale. La question des rapports entre le droit et l’anonymat reste cependant difficile tant les textes sont éparpillés et les points de vue différents, voire antagonistes. Aussi l’anonymat sur Internet est extrêmement ambivalent. Si l’idée d’un Internet entièrement anonyme peut paraître séduisante de prime abord, elle doit être mesurée et critiquée.

Partie 2. L'anonymat sur Internet : un principe non absolu et menacé

« *Il est dès lors clair que la question de l'anonymat sur l'Internet se trouve au centre d'un dilemme auquel les gouvernements et les organisations internationales doivent faire face. D'une part, la possibilité de rester anonyme est essentielle si l'on veut préserver les droits fondamentaux à la vie privée et à la liberté d'expression dans le cyberespace. D'autre part, la faculté de participer à des activités et de communiquer en ligne sans révéler son identité va à l'encontre d'initiatives lancées pour soutenir d'autres activités clés d'intérêt général tels que la lutte contre le contenu illégal et préjudiciable, la lutte contre les délits financiers ou les atteintes au droit d'auteur*[110] **».**

Dans cette logique, il convient de relire l'article 4 de la DDHC de 1789 qui dispose que « *La liberté consiste à pouvoir faire tout ce qui ne nuit pas à autrui : ainsi, l'exercice des droits naturels de chaque homme n'a de bornes que celles qui assurent aux autres Membres de la Société la jouissance de ces mêmes droits. Ces bornes ne peuvent être déterminées que par la Loi.* »

En effet, d'autres droits et libertés sont exercés sur le web par plusieurs acteurs aux objectifs différents. L'Etat a ainsi pour mission le maintient de l'ordre public et sera amené à intervenir sur Internet en vertu des textes qui l'autorisent à agir et en vertu des missions d'intérêt général qu'il assume. Certaines entreprises défendent également leurs intérêts économiques. Il est d'ailleurs notable de remarquer que parfois, le discours politique peut être largement influencé par un intérêt plus qu'un autre, ce qui représente une menace pour le droit l'anonymat (Chapitre 1).

Mais le droit, la politique et les intérêts antagonistes ne sont pas les seules limites au droit à l'anonymat. Ce droit apparaît également menacé par les développements des technologies de l'information et de la communication. L'exemple du Big Data sera adapté pour illustrer les défis que le droit doit s'apprêter à relever (Chapitre 2).

[110]Groupe de travail « *Article 29* », *Recommandation 3/97, L'anonymat sur Internet*, WP 6, 3 décembre 1997, p. 6.

Chapitre 1. Les limites à l'anonymat sur Internet

Il est en effet inconcevable aujourd'hui que l'anonymat soit juridiquement total. C'est pourquoi la loi est venue poser des limites à l'anonymat sur Internet (Section 1). La politique, en ce qu'elle précède la construction de la loi, est également un vecteur à prendre en considération afin de déceler les limites du droit à l'anonymat (Section 2).

Section 1. Les limites imposées par la loi

Dans sa décision « *Loi relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers* » du 19 janvier 2006, le Conseil Constitutionnel a considéré « *qu'il appartient au législateur d'assurer la conciliation entre, d'une part, la prévention des atteintes à l'ordre public, nécessaire à la sauvegarde de droits et de principes de valeur constitutionnelle, et, d'autre part, l'exercice des libertés constitutionnellement garanties, au nombre desquelles figurent le respect de la vie privée et la liberté d'entreprendre, respectivement protégés par les articles 2 et 4 de la Déclaration des droits de l'homme et du citoyen de 1789.* »

C'est suivant ce raisonnement que le législateur est venu limiter le principe de l'anonymat sur Internet. Les motifs invocables vont du droit des tiers à l'intérêt général. Il conviendra d'exposer comment les internautes sont identifiés et en vertu de quels textes (§1) avant de traiter des exemples d'intérêts antagonistes qui légitiment cet encadrement (§2).

§1. L'encadrement de l'identification des internautes

Dans un premier temps, il sera traité de l'identification des internautes auprès des services d'hébergement (A) puis dans un second temps de l'identification auprès des fournisseurs d'accès Internet (B).

A) L'identification des utilisateurs de services d'hébergement

Comme il a été dit plus haut, les hébergeurs ont l'obligation de détenir et conserver « *les données de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont elles sont prestataires* » en vertu de l'article 6- II alinéa 1er de la LCEN de 2004. La loi n° 2000-719 du 1er août 2000 modifiant la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication avait préalablement prévu un régime identique concernant les éditeurs à titre professionnel en son article 1er.

Pour rappel, en vertu de l'article 6- III- 2 de la LCEN, « *Les personnes éditant à titre non professionnel un service de communication au public en ligne peuvent ne tenir à la disposition du public, pour préserver leur anonymat, que le nom, la dénomination ou la raison sociale et l'adresse* [de l'hébergeur], *sous réserve de lui avoir communiqué les éléments d'identification personnelle prévus au 1.* »

Pour bénéficier de cet anonymat, les personnes physiques doivent donc communiquer à leur hébergeur « *leurs nom, prénoms, domicile et numéro de téléphone et, si elles sont assujetties aux formalités d'inscription au registre du commerce et des sociétés ou au répertoire des métiers, le numéro de leur inscription*. »

B) L'identification des abonnés à un service d'accès à Internet

L'article L. 34-1 du Code des Postes et des Communications Electroniques dispose que « *Les opérateurs de communications électroniques, et notamment les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne, effacent ou rendent anonyme toute donnée relative au trafic* » sous réserve des exceptions prévues au même article.

Les FAI sont, bien évidemment, concernés par cette disposition qui fait référence « *notamment aux personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne* ». Les abonnés bénéficient dans le cadre de ces services à la fois d'un droit à l'oubli (effacement) et d'un droit à l'anonymat qui sont de principe.

Comme il a été vu plus haut, les FAI sont soumis au décret du 25 février 2011 qui énumère les données que ces opérateurs doivent détenir et conserver pendant un délai d'un an en vertu de l'article 3 du décret.

§2. Un encadrement nécessaire au respect d'intérêts antagonistes

Afin de ne pas placer les éditeurs de contenus non professionnels en situation d'impunité de telle sorte qu'ils n'auraient à répondre des infractions qu'ils pourraient commettre, la levée de l'anonymat est possible lorsque le contenu est illégal tant au regard de la loi du 29 juillet 1881 (A) que du Code Pénal (B) et du Code la Propriété Intellectuelle (C).

Il ne sera pas traité de l'ensemble des infractions susceptibles d'être commises sur le web ayant pour conséquence une levée ou une négation de l'anonymat. Il sera présenté les

principales infractions, les principales politiques répressives qui sont en marche sur le web dont certaines sont plus acceptables que d'autres.

A) Les infractions de presse

Définies dans la loi du 29 juillet 1881 sur la liberté de la presse, les infractions de presse sont des limites légitimes à la liberté d'expression et à la liberté de communication en ligne. Ces limites se justifient notamment au moyen de la notion de droit de savoir du public. Par exemple, si la publication de nouvelles fausses est punie pénalement en vertu de l'article 27 de la loi du 29 juillet 1881 est bien une limite à la liberté d'expression c'est afin de préserver le droit de savoir du public.

Les infractions de presse sont classées par la loi du 29 juillet 1881 : les provocations aux crimes et aux délits, les délits contre la chose publique, les délits contre les personnes (injure et diffamation), les délits contre les chefs d'Etat et agents diplomatiques étrangers et enfin les publications interdites et immunités de la défense. Elles sont prévues aux articles 23 et suivants de la loi de 1881.

L'ensemble de ces infractions est susceptible de provoquer une levée de l'anonymat des éditeurs de contenu à titre non professionnel prévu par la LCEN. L'identification de l'auteur de propos réprimés par la loi 29 juillet 1881 sera en réalité assez aisée. Les personnes s'estimant victimes pourront déposer plainte avec constitution de partie civile. Le juge d'instruction pourra ainsi confier à un service de police la mission de contacter l'hébergeur, dont la dénomination ou la raison social et l'adresse doivent figurer dans les mentions légales du site édité anonymement[111], afin qu'il leur communique l'identité de l'éditeur du site par réquisition judiciaire.

Aussi, le ministère public pourra déclencher l'action publique s'il estime un contenu illégal. A noter que dans le cas où le texte litigieux a été laissé par un destinataire du service, comme par exemple un commentateur anonyme, il suffit aux services de police de demander à l'éditeur les données de connexion de l'internaute en question (heure de connexion et adresse IP), contacter le FAI correspondant à l'adresse IP communiquée qui leur donnera les coordonnées de l'abonné qui utilisait cette adresse IP à la date et à l'heure de l'édition du

[111] *Loi pour la confiance dans l'économie numérique*, n° 2004-575, 21 juin 2004, art. 6, III, 2. Cette obligation est pénalement sanctionnée d'un an d'emprisonnement et de 75000 euros d'amende par l'article 6, VI, 2 de la même loi.

texte. Cette procédure reste marginale dans la mesure où, grâce au système de signalement, l'éditeur peut retirer promptement un contenu manifestement illicite.

L'identité de l'éditeur de contenus non professionnels sera constituée de son nom, prénoms, domicile et numéro de téléphone, conformément à l'article 6- III- 1- a) de la LCEN de 2004.

Twitter a récemment été impliqué dans une affaire de droit de la presse. Plusieurs « *tweets* »[112] antisémites ainsi que les « *hashtags* »[113] idoines (#unbonjuif, #unjuifmort…) ont été publiés par des utilisateurs anonymes de Twitter. Des associations de lutte contre le racisme, après s'être heurtées au refus du réseau social de retirer les contenus en cause, ont assigné Twitter devant le Tribunal de Grande Instance de Paris qui a rendu une ordonnance de référé obligeant Twitter à communiquer aux requérants les données permettant « *l'identification de quiconque a contribué à la création des tweets manifestement illicites* »[114].

Ces données sont donc communicables aux requérants dans le but qu'ils assignent les bonnes personnes devant le justice afin de faire valoir leurs droits par le biais d'une citation directe devant un tribunal correctionnel. Cette exemple illustre une limite légitime à l'anonymat que le législateur est en droit d'imposer.

B) La lutte contre la pédopornographie

L'article 227-23 du Code pénal incrimine « *Le fait, en vue de sa diffusion, de fixer, d'enregistrer ou de transmettre l'image ou la représentation d'un mineur lorsque cette image ou cette représentation présente un caractère pornographique* » de même que « *Le fait d'offrir, de rendre disponible ou de diffuser une telle image ou représentation, par quelque moyen que ce soit, de l'importer ou de l'exporter, de la faire importer ou de la faire exporter, est puni des mêmes peines*. » La peine est aggravée « *lorsqu'il a été utilisé, pour la diffusion de l'image ou de la représentation du mineur à destination d'un public non déterminé, un réseau de communications électroniques* » et s'élève à 7 ans d'emprisonnement et à 100 000 euros d'amende.

[112] Les tweets sont des messages courts (maximum 140 caractères) édités par les utilisateurs de Twitter.
[113] Un hashtag est en réalité le symbole « # » utilisé sur Twitter comme un mot-clef.
[114] TGI Paris, ord. de référé, 24 janvier 2013, [http://www.pcinpact.com/news/77023-exclusif-telecharger-ordonnance-refere-uejf-contre-twitter.htm].

L'article 6- I- 7 alinéa 3 fait écho à cette infraction en disposant que « *Compte tenu de l'intérêt général attaché à la répression de l'apologie des crimes contre l'humanité, de l'incitation à la haine raciale ainsi que de la pornographie enfantine,* [hébergeurs et FAI] *doivent concourir à la lutte contre la diffusion des infractions visées* […] *à l'article 227-23 du code pénal*. »

Ici, la lutte contre la pédopornographie est rattachée à la notion d'intérêt général afin de justifier les limites imposées à la liberté de communication en ligne. Le même article ajoute : « *A ce titre, elles doivent mettre en place un dispositif facilement accessible et visible permettant à toute personne de porter à leur connaissance ce type de données. Elles ont également l'obligation, d'une part, d'informer promptement les autorités publiques compétentes de toutes activités illicites mentionnées à l'alinéa précédent qui leur seraient signalées et qu'exerceraient les destinataires de leurs services, et, d'autre part, de rendre publics les moyens qu'elles consacrent à la lutte contre ces activités illicites*. »

A la lecture de cette disposition, l'anonymat trouve sa limite dans la collaboration nécessaire qu'entretiennent l'autorité publique et les FAI et les hébergeurs et qui s'inscrit dans un intérêt général expressément mentionné par le législateur.

C) La lutte contre la contrefaçon sur Internet

C'est à partir de 2009 que la lutte contre la contrefaçon a pris une nouvelle dimension. Avec le développement des technologies du « *peer to peer* », du « *direct download* » et du « *streaming* », la contrefaçon est devenue un phénomène international. C'est, de plus, une problématique largement médiatisée.

Le rejet de l'*Anti Counter-Feiting Trade Agreement*[115] (ACTA) par le Parlement européen le 4 juillet 2012 a été largement relayé dans la presse traditionnelle[116] bien que sa nouvelle forme, le projet TAFTA (*Trans-Atlantique Free Trade Agreement*)[117] soit restée un peu plus dans l'ombre. Egalement, le sujet est si sensible que même les projets de loi étrangers relatifs à la lutte contre la contrefaçon animent le débat en France et en Europe

[115] En français : « Accord Commercial Anti-Contrefaçon ».
[116] Renaud HONORE, « Le Parlement européen enterre définitivement ACTA », Les Echos, 5 juil. 2012, [http://www.lesechos.fr/05/07/2012/LesEchos/21220-092-ECH_le-parlement-europeen-enterre-definitivement-acta.htm?texte=pipa] ; Damien LELOUP, « Le Parlement européen vote contre le traité anticontrefaçon ACTA », Le Monde, 4 juil. 2012, [http://www.lemonde.fr/technologies/article/2012/07/04/le-parlement-europeen-vote-contre-le-traite-anti-contrefacon-acta_1729032_651865.html?xtmc=acta&xtcr=7].
[117] En français : « Accord de libre échange Transatlantique ».

comme par exemple les projets SOPA (*Stop Online Piracy Act*)[118], PIPA (*Protect IP Act*)[119] et CISPA (*Cyber Intelligence Sharing and Protection Act*)[120] déposés à la Chambre des représentants aux Etats-Unis[121].

La répression des atteintes au droit d'auteur et aux droits voisins est de plus en plus mal vécue par la société civile numérique. Cette lutte s'accompagne en réalité d'une surveillance de plus en plus accrue des internautes. Ce constat a conduit à l'amorce d'une mobilisation citoyenne qui se pose en droite ligne au modèle économique du droit d'auteur actuel tel un alter mondialisme numérique[122]. Ce phénomène a aussi impacté les acteurs de l'économie culturelle qui commencent à développer des alternatives toutes rangées sous l'expression générique « offre légale ». Aussi, le financement de la culture est en pleine évolution et de nouveaux modèles économiques se développent, tel que le « *crowd founding* »[123].

C'est avec les lois HADOPI 1 et 2 des 12 juin et 28 octobre 2009 que la France entre de plein pied et avec précipitation dans la lutte contre la contrefaçon sur Internet. La Haute Autorité pour la Diffusion des Œuvres et la Protection des Droits sur Internet (HADOPI), partiellement remise en cause par le récent « Rapport Lescure »[124], est ainsi prévue à l'article L. 331-12 du CPI.

La HADOPI assure une « *mission de protection de ces œuvres et objets à l'égard des atteintes à ces droits commises sur les réseaux de communications électroniques utilisés pour la fourniture de services de communication au public en ligne* »[125].

Ses membres « *peuvent, pour les nécessités de la procédure, obtenir tous documents, quel qu'en soit le support, y compris les données conservées et traitées par les opérateurs de communications électroniques en application de l'article L. 34-1 du code des postes et des communications électroniques et les prestataires mentionnés aux 1 et 2 du I de l'article 6 de*

[118] En français : « Loi contre le piratage en ligne ».
[119] En français : « Loi sur la prévention des menaces en ligne réelles sur la créativité économique et le vol de la propriété intellectuelle ».
[120] En français : « Loi sur le partage et la protection des informations en ligne ».
[121] Xavier BERNE, « Après SOPA et PIPA, la menace CISPA », PC Impact, 6 avr. 2012, [http://www.pcinpact.com/news/70073-cispa-sopa-pipa-congres-rogers.htm].
[122] Comme la Quadrature du Net, le Parti Pirate, les Robins du Web, la NURPA, l'Electronic Frontier Foundation aux Etas-Unis…
[123] En français : « financement par le public ».
[124] Rendu en mai 2013, ce rapport propose entre autre de transférer les compétences et missions de l'HADOPI au Conseil supérieur de l'audiovisuel.
[125] *Code de la propriété intellectuelle*, art. L. 331-13, 2°.

la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique [c'est-à-dire les hébergeurs et les FAI à titre principal] » ainsi qu'une copie de ces documents[126].

Les membres peuvent également « *obtenir des opérateurs de communications électroniques l'identité, l'adresse postale, l'adresse électronique et les coordonnées téléphoniques de l'abonné* » dont l'accès à des services de communication au public en ligne a été utilisé à des fins de contrefaçon[127].

A la simple lecture de ces dispositions, il est clair que le législateur a clairement arbitré le conflit entre le bloc « respect de la vie privée/liberté de communication en ligne » et le bloc « droit d'auteur/droit de propriété » en faveur de ce dernier.

L'article L. 331-29 du CPI a ouvert la possibilité de créer un traitement de données à caractère personnel ayant pour finalité « *la mise en œuvre, par la commission de protection des droits, des mesures prévues à la présente sous-section, de tous les actes de procédure afférents et des modalités de l'information des organismes de défense professionnelle et des sociétés de perception et de répartition des droits des éventuelles saisines de l'autorité judiciaire ainsi que des notifications prévues au cinquième alinéa de l'article L. 335-7.* »

Le décret pris en Conseil d'Etat n° 2010-236 du 5 mars 2010 relatif au traitement automatisé de données à caractère personnel autorisé par l'article L. 331-29 du Code de la Propriété Intellectuelle dénommé « Système de gestion des mesures pour la protection des œuvres sur internet » est venu préciser les modalités ouverte par l'article L.331-29 du CPI.

L'article 8 du décret prévoit deux interconnexions avec ce traitement. La première se fait avec « *les traitements automatisés de données à caractère personnel mis en œuvre par les organismes de défense professionnelle régulièrement constitués, les sociétés de perception et de répartition des droits, le Centre national du cinéma et de l'image animée* » et la deuxième avec « *les traitements mis en œuvre par les opérateurs de communications électroniques* ».

En somme, le pouvoir de « police administrative numérique » est partagé avec, entre autres, les représentants des ayants droit et les syndicats de défense des artistes ainsi qu'avec les FAI. Il résulte de l'annexe 1 du décret que les données personnelles que pourront collecter les représentants des ayants droit sont la date et heure des faits, l'adresse IP des abonnés concernés, le protocole pair à pair utilisé, le pseudonyme utilisé par l'abonné, des informations

[126] *Code de la propriété intellectuelle*, art. L. 331-21, al. 3 et al. 4.
[127] *Code de la propriété intellectuelle*, art. L. 331-21, al. 5.

relatives aux œuvres ou objets protégés concernés par les faits, le nom du fichier tel que présent sur le poste de l'abonné (le cas échéant), le FAI auprès duquel l'accès a été souscrit.

Les FAI, quant à eux, collectent pour le compte de la HADOPI les données suivantes : le nom de famille, les prénoms, l'adresse postale et les adresses électroniques, les coordonnées téléphoniques, l'adresse de l'installation téléphonique de l'abonné.

La lecture de ces dispositions éclaire encore plus l'arbitrage entre les deux blocs qu'a opéré le législateur. C'est la loi n° 2004-801 du 6 août 2004 modificatrice de la loi informatique et libertés qui est venue ouvrir la possibilité pour les sociétés de perception et de répartition des droits d'auteur et des droits des artistes-interprètes et des producteurs de phonogrammes et de vidéogrammes ainsi que les organismes de défense professionnelle de mettre en œuvre des traitements de données à caractère personnel relatives aux infractions[128].

Le Conseil Constitutionnel n'a pas considéré que ce mécanisme portait une atteinte disproportionnée l'article 2 de la DDHC de 1789 qui implique le droit au respect de la vie privée[129]. On pourrait objecter à cette décision un raisonnement découlant de la lecture combinée des articles 12 et 16 de la DDHC de 1789 et de l'article 66 de la Constitution de 1958.

L'article 12 de la DDHC dispose que « *La garantie des droits de l'Homme et du Citoyen nécessite une force publique : cette force est donc instituée pour l'avantage de tous, et non pour l'utilité particulière de ceux auxquels elle est confiée*. » Si on considère que les sociétés qui représentent les ayants droit et les organismes de défense professionnelle sont avantagés par cette mise en place d'un traitement de données personnelles qui peut se comparer à une mission de police administrative, ce mécanisme serait contraire à cette disposition. Aussi, l'article 16 de la DDHC qui dispose que « *Toute Société dans laquelle la garantie des Droits n'est pas assurée, ni la séparation des Pouvoirs déterminée, n'a point de Constitution* » pourrait permettre d'exclure les personnes privées de ce mécanisme car elles ne sont délégataires ni du pouvoir exécutif, ni du législatif, ni du judiciaire. Enfin, l'article 66 de la Constitution qui dispose que l'autorité judiciaire est gardienne de la liberté individuelle permettrait peut-être de censurer ce dispositif dans lequel le juge judiciaire n'intervient pas et est remplacé par la commission des droits de la HADOPI.

---

128 *Loi relative à l'informatique, aux fichiers et aux libertés*, n° 78-17, 6 jan. 1978, art. 9, 4°.

129 Cons. const., 10 juin 2009, n° 2009-580 DC, *Loi favorisant la diffusion et la protection de la création sur interne*, cons. 27.

Le Conseil d'Etat a considéré le décret n° 2010-236 du 5 mars 2010 relatif au traitement automatisé « HADOPI » conforme à la loi mais sans se poser la question de la légalité de l'interconnexion[130]. Peut-être en aurait-il été autrement si la critique du décret avait été faite à travers le prisme de la notion de police administrative. Il est de jurisprudence constante que le pouvoir de police administrative ne peut être délégué ou concédé, de sorte qu'aucun acte administratif ou contrat administratif ne peut disposer de cette activité régalienne au bénéfice d'une personne privée[131]. Mais la loi écran empêche ce raisonnement.

Mais quelles sont les conséquences de ce régime sur l'anonymat ? Le constat est simple : la surveillance du web est assez poussée en France. Ce type d'atteinte à la vie privée est vécu comme un retour du totalitarisme par certains. Sans tomber dans de telle extrémités, c'est à la politique constitutionnelle de réévaluer son arbitrage entre le bloc « respect de la vie privée/liberté de communication en ligne » et le bloc « droit d'auteur/droit de propriété » même si, dès 2004, le Conseil avait déjà opéré un tel arbitrage[132]. Le système d'information HADOPI permettant une identification directe (par la commission de protection des droits et les FAI) et indirecte (par les sociétés de perception de droits et les organismes de défense professionnelle) représente une réelle atteinte à l'identité des personnes. Ici, l'anonymat des internautes n'existe pas ou constitue une exception rare. Le FAI, en vertu de l'article L.34-1, III du Code des postes et des communications électroniques, pourra en effet être contraint de différer d'un an les opérations consistant à effacer ou rendre anonymes certaines données techniques.

La lutte contre la contrefaçon a pris des proportions assez démesurées quand on voit que, très régulièrement, les personnes, surtout les publics jeunes, téléchargent des contenus disponibles sur le web avec une facilité déconcertante. Mais comment résister à une offre culturelle si facilement accessible ? Les habitudes de consommation culturelle sont en train de changer de manière irréversible. Ce n'est pas vers un « tout répressif » à l'égard des personnes que les juristes et les opérateurs culturels doivent se pencher mais bien vers des modèles alternatifs où chacun trouve son avantage.

[130] CE, sect., 19 oct. 2011, *French Data Network*, n° 339279.
[131] CE, 17 juin 1932, *Ville de Castelnaudary*, Lebon p. 595, concl. JOSSE.
[132] Cons. Const., 29 juillet 2004, n° 2004-499 DC, *Loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*.

Mais les tempéraments à l'anonymat ne sont pas seulement le fait du droit. Certaines limites trouvent leur source dans le discours politique et la souveraineté des Etats ou les intérêts de certaines entreprises.

Section 2. Les objections politiques à l'anonymat sur Internet

Internet a commencé à se développer sans une régulation très poussée de la part des Etats au point qu'il a pu être qualifié de « nouveau continent ». Aujourd'hui, le web est de plus en plus régulé mais mieux sécurisé juridiquement. Mais il reste cependant des failles qui sont exploitées au détriment des plus vulnérables.

Que ce soit en France ou à l'étranger, que ce soit le secteur public ou le secteur privé, on assiste à un recul de la considération de la vie privée et de l'anonymat des personne. L'anonymat étant un droit par défaut (préalable à tout traitement de données), les empiètements sur ce droit se font, et c'est regrettable, bien souvent pour des motifs très vagues et dont le bien fondé reste difficilement vérifiable. Au Japon, le système de navigateur TOR, qui permettait en théorie une navigation anonyme, vient d'être interdit sur les recommandations du ministère de l'intérieur japonais [133] au motif d'abus. Mais faut-il interdire, suivant cette logique, la totalité du web au motif que des abus peuvent-être commis ?

Benjamin Franklin disait « *Un peuple prêt à sacrifier un peu de liberté pour un peu de sécurité ne mérite ni l'une ni l'autre, et finit par perdre les deux*. » Influencé par l'esprit des Lumières, cette phrase de Franklin nous invite à nous indigner contre l'arbitraire, d'où qu'il vienne, et de donner à la liberté la place fondamentale qu'elle mérite.

Afin d'illustrer cette idée, nous exposerons plusieurs exemple. Bien qu'il semble acquis, l'anonymat de l'expression instauré en 2004 n'est pas à l'abri de certains discours politiques (§1). De même, la faculté des entreprises à défendre leurs intérêts économiques auprès d'instances démocratiques est très dangereuse pour les droits des internautes (§2). Enfin, il est nécessaire de porter notre attention sur les conséquences que peuvent provoquer les dérives sécuritaires sur le droit à l'anonymat (§3).

[133] Guénaël PEPIN, « La police japonaise recommande le blocage du réseau TOR », Le Monde, 23 avr. 2013, [http://www.lemonde.fr/technologies/article/2013/04/23/la-police-japonaise-recommande-le-blocage-du-reseau-tor_3164344_651865.html].

§1. La remise en cause de l'anonymat de l'expression en France

Le sénateur Jean-Louis Masson est à l'origine d'une proposition de loi « *tendant à faciliter l'identification des éditeurs de sites de communication en ligne et en particulier des «blogueurs » professionnels et non professionnels* » enregistrée au bureau du Sénat depuis 2010[134].

L'exposé des motifs nous donne un éclairage sur les motivations d'une telle proposition. Tout en reconnaissant que le régime instauré par la LCEN est globalement positif, le sénateur invoque, pour se justifier, les dérives qu'ont pu entraîner un tel régime. La logique serait donc d'imposer une identification des blogueurs visible du public à cause d'une poignée de blogueurs qui commettent des actes d'injure, de diffamation, de dénigrement ou autres.

Un tel pas en arrière serait très préjudiciable pour la société civile qui serait moins incitée à créer du contenu sur Internet, à prendre la parole et à contribuer aux débats. Nous connaissons tous les dérives choquantes des commentaires sous des articles ou vidéos en ligne. Internet a cette particularité de cristalliser tout les travers de la société (diffamations, injures, pédophilie, fraude au droit d'auteur). Cependant, il existe très certainement un phénomène d'autorégulation. Même si les internautes ne sont pas une « masse consciente », on peut constater qu'un tri se fait de lui-même.

Dans un article intitulé « De la valeur du pseudonymat aux dangers de l'identité réelle unifiée », Hubert Guillaud bat en brèche l'argument classique selon lequel l'anonymat ou le pseudonymat induisent un contenu de moins bonne qualité[135]. Se fondant sur une étude réalisée par le site « Disqus.com »[136], l'étude révèle que l'usage du pseudonyme par les internautes implique une plus grande participation aux discussions ainsi qu'un contenu jugé par les pairs comme de meilleure qualité. Bien qu'une telle étude soit scientifiquement lacunaire, l'expérience d'Internet nous conduit à en approuver le résultat.

---

[134] *Proposition de loi tendant à faciliter l'identification des éditeurs de sites de communication en ligne et en particulier des « blogueurs » professionnels et non professionnels*, n° 423, 3 mai 2010, [http://www.senat.fr/leg/ppl09-423.html].

[135] Hubert GUILLAUD, « De la valeur du pseudonymat aux dangers de l'identité réelle unifiée », InternetActu, 25 jan. 2012, [http://www.internetactu.net/2012/01/25/de-la-valeur-du-pseudonymat-aux-dangers-dune-identite-reelle-unifiee/].

[136] [http://disqus.com/research/pseudonyms/].

C'est ce phénomène qui justifie le régime de l'anonymat fixé par le législateur de 2004. Revenir sur un tel régime reviendrait à priver les citoyens du droit de prendre la parole, de nier leur liberté d'expression et de communication en ligne.

De plus, les voies de droit pour sanctionner les abus comme les injures, la diffamation ou le dénigrement existent et sont efficaces pour peu que l'hébergeur coopère et que les informations que l'éditeur de contenu non professionnel soient exactes. La possibilité pour le pouvoir judiciaire de faire bloquer ou d'imposer le retrait en urgence d'un contenu illicite répond à l'exigence de garantie des droits des tiers.

Pour finir, il semble peu probable que cette proposition de loi soit un jour mise en débat vu l'ancienneté du dépôt (2010) et en dépit de récentes offensives[137]. Mais si ce projet de loi semble avoir peu de chances de sortir des étagères du Sénat, d'autres règlementations à l'origine très favorables aux droits des internautes risquent de subir des dénaturations importantes.

§2. Le lobbying au Parlement européen : une menace pour les droits des internautes

Les géants du Net ne s'en cachent presque pas. Ne voyant pas d'un bon œil certaines dispositions du futur règlement général sur la protection des données personnelles, estimant sans doute que les obligations qui pourront leur être imposées sont trop contraignantes.

Le site internet d'open data « lobbyplag.eu »[138] propose de manière entièrement gratuite un comparateur d'amendements et de suggestions d'amendement des différents lobbys actifs au Parlement européen sur le débat autour du projet de règlement. Certaines constatations sont navrantes : certaines suggestions faites par des lobbys ne sont pas retouchées par les parlementaires européens et sont susceptibles d'être soumises au vote telles quelle !

Parmi ces lobbys, on retrouve des acteurs tels qu'Amazon, eBay, la Chambre de commerce américaine, Facebook, Google ou encore Yahoo !.

[137] Julien L., « L'anonymat des blogueurs une nouvelle fois sur la sellette », Numerama, 27 fév. 2013, [http://www.numerama.com/magazine/25232-l-anonymat-des-blogueurs-une-nouvelle-fois-sur-la-sellette.html].
[138] [http://lobbyplag.eu/lp].

La Quadrature du Net a réussi à se procurer les recommandations de Facebook sur le projet de règlement[139]. Facebook y émet plusieurs remarques, notamment à propos de l'application territoriale du texte. La firme a en effet intérêt à maintenir le statu quo et à continuer de bénéficier de la clémence de la Commission européenne à propos du « *Safe Harbor* »[140] qui permet aux géants du net américains de se soumettre à une version bien plus souple de la directive de 1995 et dont le respect est contrôlable en interne.

Le lobbying peut paraître insupportable et provoquer l'indignation. Rappelons toutefois qu'il existe également des lobbys agissant en faveur de la protection des données et de la vie privée[141]. Cependant, la différence des moyens financiers entre un géant d'Internet et une association de défense des droits et libertés des internautes est tellement profonde qu'on ne peut être que très pessimiste sur l'équilibre du rapport de force. Ce manque de transparence est très dangereux pour la démocratie européenne déjà fortement contestée.

On peut donc s'attendre à un texte complètement miné, dénaturé, et à de plus en plus d'intrusion dans notre vie privée. Le niveau de sécurité juridique, déjà très bas à l'heure actuelle, risque fortement d'être proportionnellement atteint. L'anonymat apparaît être une chimère et l'identification à outrance une réalité. L'intérêt économique ne permet pas toutes les largesses avec la vie privée et l'identité des personnes, en principe, dans une démocratie qui garantie le respect de la vie privée[142].

§3. La sécurité : fondement légitime de l'atteinte aux libertés et à l'identité des personnes ?

Que ce soit aux Etats-Unis avec le célèbre « *USA Patriot Act* » de 2001 ou le « *Foreign Intelligence Surveillance Act of 1978 Amendments Act* » (FISAAA) de 2008, ou en France avec la loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure (LOPPSI 2), les puissances mondiales accentuent de plus en plus leur contrôle et leur régulation sur le web. Bien évidemment, la souveraineté d'un Etat implique que celui-ci assure le maintient de l'ordre public. En France, le triptyque classique de l'ordre public implique la salubrité, la tranquillité mais surtout la sécurité. Toutefois, sans

[139][http://www.laquadrature.net/wiki/images/3/3b/20121026_Drafting-recommendations_IMCO-draft-opinion_final.pdf].
[140] En français : « Sphère de sécurité ». Le Safe Harbor, déclaré conforme par la Commission européenne afin d'autoriser les transferts de données aux Etats-Unis, énonce des principes à respecter par les responsables de traitements américains.
[141] Mais à la différence des lobbys « classiques », ceux-ci défendent l'intérêt général, pas des intérêts privés.
[142] Charte des droits fondamentaux de l'Union européenne, 2000/C 364/01, 7 décembre 2000, art. 7.

remettre en cause cet objectif d'intérêt général, il devient évident que l'avenir de nos démocraties dépend de la juste appréciation de l'équilibre entre liberté et sécurité.

Les garanties juridiques des droits et libertés sont désormais mises à l'épreuve de l'internationalisation des échanges couplée à l'internationalisation de la criminalité et du terrorisme.

A titre d'exemple, il est nécessaire de lire l'article 11 de la LOPPSI 2 qui prévoit un fichier d'analyse sérielle, c'est-à-dire un traitement de données personnelles, enregistrant les personnes à l'encontre lesquelles « *il existe des indices graves ou concordants rendant vraisemblable qu'elles aient pu participer, comme auteurs ou complices, à la commission d'une infraction mentionnée au 1° de l'article 230-12* » du Code de procédure pénale, ou même celles « *A l'encontre desquelles il existe des raisons sérieuses de soupçonner qu'elles ont commis ou tenté de commettre une infraction mentionnée au 1° du même article 230-12* ». Ce traitement étant consultable par les services de police, les magistrats du parquet, les magistrats instructeurs et les services de douane, on constate que le pouvoir administratif empiète sur le pouvoir judiciaire qui intervient ici de manière résiduelle en la personne du juge d'instruction. Un tel traitement sera alimenté et consulté par les services de police à charge, mais on imagine mal des éléments collectés à décharge vu l'opacité qui entoure un tel traitement.

On peut donc imaginer le déséquilibre opéré par un tel traitement, alimenté par des données personnelles glanées sur Internet, au détriment des droits de la défense. L'automatisation des enquêtes représente à ce titre une réelle inquiétude.

Mais c'est surtout le filtrage d'Internet qui induit le plus de questions. L'interconnexion des fichiers de l'administration avec ceux prévus par le Code de la Propriété Intellectuelle et ceux prévus par le Code des Postes et des Communications Electronique, avec l'archivage que cela implique, est très délicat. Il en est de même avec l'obligation qui est faite aux hébergeurs et FAI d'« *d'informer promptement les autorités publiques compétentes de toutes activités illicites mentionnées à l'alinéa précédent qui leur seraient signalées et qu'exerceraient les destinataires de leurs services* » en vertu de l'article 6, I, 7 de la LCEN.

En juin 2013, le journal britannique The Guardian révèle au public l'existence d'un programme du nom de « PRISM » instaurant une étroite collaboration entre la *National*

Security Agency (NSA) américaine et quelques grandes entreprises du web[143]. Bien que les faits de cette affaire restent encore flous, il apparaîtrait que des agents puissent accéder aux serveurs de grandes sociétés comme Facebook, Youtube, Google ou Skype sur le fondement du paragraphe 1881 du FISAAA qui autorise, sans mandat, l'écoute et la consultation des communications électroniques de personnes résidants hors des Etats-Unis. Google a par ailleurs publié quelques informations sur la surveillance opérés par les services américains sur les comptes d'utilisateurs français[144].

Cette affaire illustre bien le manque de contrôle et de garanties juridiques dont nous disposons. Le droit d'opposition, qui est une manifestation du droit à l'anonymat, n'existe bel et bien pas sur Internet. Le droit au consentement est ici largement bafoué par l'opacité volontairement maintenue. Seule une réponse internationale pourrait palier à cette carence. La Commission Européenne a d'ailleurs commencé à réagir et demande des explications à Washington[145].

Le droit de ne pas être reconnu est donc sérieusement mis à mal à travers ces différents exemples. Les Etats ainsi que certaines entreprises ne semblent pas encore mesurer les atteintes disproportionnées qui sont portées aux droits et libertés des individus. De surcroît, les développements technologiques doivent prendre en compte ce facteur déterminant. La pérennité et la confiance en Internet dépend en effet d'un développement respectueux de la vie privée des personnes.

[143] Glenn, GREENWALD, « NSA Prism program taps in to user data of Apple, Google and others », The Guardian, 7 juin 2013, [http://www.guardian.co.uk/world/2013/jun/06/us-tech-giants-nsa-data].
[144] [http://www.google.com/transparencyreport/userdatarequests/FR/].
[145] Renaud HONORE, « PRISM : Bruxelles demande des explications à Washington », Les Echos, 11 juin 2013, [http://www.lesechos.fr/economie-politique/monde/actu/0202821199298-bruxelles-preoccupe-au-plus-haut-niveau-par-l-affaire-prism-574351.php].

Chapitre 2. L'anonymat, principe menacé par les développements technologiques : l'exemple du Big Data

En effet, certaines innovations web et certaines dérives semblent mettre à mal l'anonymat et la vie privée des individus. Ces innovations vont sans doute accentuer les difficultés juridiques inhérentes à Internet, c'est pourquoi il est nécessaire d'instaurer des règles efficaces afin d'assurer la sécurité juridique des personnes. Il en dépend de la confiance des individus lorsqu'ils naviguent sur Internet.

L'exemple du Big Data est, à ce titre, l'exemple le plus intéressant tant les implications sociétales et juridiques qu'il suppose sont vastes et imprévisibles (Section 1). C'est pourquoi il sera nécessaire de se poser la question d'un cadre juridique applicable au Big Data afin de préserver la vie privée et l'identité des personnes (Section 2).

Section 1. La mutation de la société par le Big Data

Avant tout développement sur les relations ambivalentes de la notion de Big Data et du droit (§2), il conviendra d'essayer de définir les contours du Big Data et d'évoquer les changements sociétaux que ce phénomène implique (§1).

§1. La révolution du Big Data

Dans un article passionnant, Hubert Guillaud traite du Big Data et du très probable changement de paradigme qu'il va opérer[146]. Véritable chamboulement de la société et des rapports humains, le Big Data peut légitimement faire peur en ce qu'il est impossible de prévoir ou d'imaginer tout les potentiels qu'il présente. C'est une véritable réflexion sur le progrès qui s'impose à nous.

Mais comment définir le Big Data ? La question est complexe et la définition que nous proposons est sans doute lacunaire. Le Big Data serait le processus permettant une agrégation et un croisement massif de données, à une échelle dont les proportions vont au-delà de l'imagination de tout esprit humain. Le Big Data pose à la fois un problème de stockage et le cloud computing peut alors apparaître comme une solution mais aussi un problème éthique. Hubert Guillaud suppose même que l'adage de Lessig « *code is law* » perdrait tout son sens dans ce processus car les algorithmes et codes sources deviendront trop complexes. L'enjeu d'un tel processus est avant tout l'anticipation et la prédictibilité des faits sociaux,

[146] Hubert GUILLAUD, « Big Data : nouvelle étape dans l'informatisation du monde », InternetActu, 14 mai 2013, [http://www.internetactu.net/2013/05/14/big-data-nouvelle-etape/].

économiques, voir juridique. Par exemple, il sera possible de prévoir des carrières, des crises financières, des épidémies, des manifestations, des guerres et pourquoi pas des décisions de justice sans pouvoir retracer un cheminement compréhensible pour l'humain ou par un ordinateur. Quand la prédictibilité est imprévisible.

Plus philosophiquement, Hubert Guillaud pose plusieurs questions légitimes : « *Quel rôle sera laissé à l'intuition, à la foi, à l'incertitude, à notre libre arbitre, à notre liberté à agir en contradiction avec les preuves, à l'apprentissage par l'expérience ? A l'heure des corrélations, que va devenir notre idéal, notre capacité à toujours chercher la causalité ? Assurément, nos certitudes sur ce que nous sommes sont appelées à changer*. »

L'esprit humain et les rapports sociaux sont amenés à être remis en question. Il sera bien évidemment nécessaire que le droit s'adapte tant les incidences possibles sont nombreuses et tant cette révolution est imminente. Les droits et libertés des personnes apparaissent bien fragiles face à un tel phénomène, a fortiori le droit à l'anonymat.

§2. Les incidences possibles sur le droit et sur l'anonymat des personnes

Il conviendra avant tout d'évoquer les incidences possibles du Big Data sur le droit en général (A) puis sur l'anonymat des personnes (B).

A) Des incidences incertaines sur le droit

On peut imaginer plusieurs incidences du Big Data sans toutefois embrasser toutes les possibilités. Que deviendront le principe de la présomption d'innocence, la souveraineté des Etats, la liberté d'entreprendre, le secret professionnel, le secret des correspondances, la liberté contractuelle, la gestion des risques dans les contrats, les principes d'égalité et de liberté, la liberté d'aller et venir ? Ces notions jetées en pagaille sont toutes potentiellement remises en question.

C'est en se posant ce genre de questions que l'article 10 de la loi informatique et libertés qui dispose qu' « *Aucune décision de justice impliquant une appréciation sur le comportement d'une personne ne peut avoir pour fondement un traitement automatisé de données à caractère personnel destiné à évaluer certains aspects de sa personnalité* » et qu' « *Aucune autre décision produisant des effets juridiques à l'égard d'une personne ne peut être prise sur le seul fondement d'un traitement automatisé de données destiné à définir le profil*

de l'intéressé ou à évaluer certains aspects de sa personnalité » prend une tournure particulièrement solennelle.

Il est donc impératif de donner pleinement son sens à cette disposition. Ici aussi, l'insécurité juridique doit être limitée le plus possible même si les moyens de droit pour y arriver ne sont pas simples à déterminer.

B) Des incidences mettant en péril l'anonymat

L'informaticien Arvin Narayanan de l'Université de Princeton a pu écrire qu'à l'heure du Big Data « *l'anonymat est devenu algorithmiquement impossible* »[147].

En effet, l'éparpillement des données personnelles que nous évoquions plus haut va s'accentuer de manière exponentielle tandis que notre contrôle sur ces données baissera proportionnellement[148]. Les droits des personnes fichées garantis des par la directive de 1995, la loi informatique et libertés et le futur règlement général seront réduis à peau de chagrin. Hubert Guillaud évoque le dépassement des notions de consentement préalable, d'*opt out* et d'anonymisation.

Le raisonnement est simple. Il deviendra impossible de demander le consentement de la personne pour tous les traitements secondaires et non initialement prévus. De même, l'anonymisation deviendra impossible si on prend en considération l'ensemble des moyens de ré-identification possible et du nombre de données que nous sommes amenés à produire à travers les réseaux sociaux, la géolocalisation et de manière général à travers l'augmentation des échanges dû au Big Data. Le développement des « *tags* » sur Internet, qui permettent à n'importe quel éditeur de contenu ou internaute d'identifier une personne ou un contenu, est une manifestation de cet accroissement des échanges.

Des concepts tels que le *privacy by design*, la portabilité des données ou la transparence ou toute autre mesure destiné à prévenir les atteintes à l'identité ou à la vie privée seront remises en cause tant les algorithmes sont amenés à se complexifier et les sources à se diversifier. A fortiori, il sera de plus en plus difficile d'exercer un droit à consentir car on peut imaginer que des notions comme l'intérêt légitime du responsable du

[147] *Ibid*.
[148] On peut à titre d'exemple évoquer l'affaire du moteur de recherche de données personnelles « Riot » qui permettait entre autre de visualiser des données de géolocalisation, des photos et autres informations sur n'importe qui : [http://www.01net.com/editorial/586581/riot-le-moteur-de-recherche-qui-espionne-votre-vie-privee-en-ligne/].

traitement seront interprétées encore plus largement ou bien impossible à en vérifier le bien fondé.

Si on considère que le droit à l'anonymat trouve son essence dans le droit d'opposition, comment une telle opposition serait possible dans une société dans laquelle ne seront « contraints » par la force des choses d'utiliser les réseaux actuels et futurs, exercer notre liberté de communication en ligne, et donc de produire des données ?

Devant ces prédications un peu alarmantes, il convient néanmoins d'entamer une réflexion juridique autour du Big Data.

Section 2. Quel cadre juridique pour l'anonymat dans le contexte du Big Data ?

Selon Hubert Guillaud, l'évolution du droit dans le cadre du Big Data passe par la responsabilisation des entreprises qui utilisent ce procédé. Cette idée renvoie directement au concept d'*accountability* qui a été exposé plus haut.

En effet, il est envisageable de contraindre les entreprises qui utilisent du Big Data a rapporter la preuve du respect de l'ensemble des dispositions du règlement tel que l'impose l'article 5, f) du projet de règlement général. L'article 22 instaure à ce titre une obligation d'établir des règles internes et de définir des mesures appropriées afin de garantir et démontrer le respect du règlement, notamment sur le recensement des traitements, l'obligation de sécurité, l'accomplissement des formalités préalables et la désignation d'un correspondant à la protection des données. Le 3 du même article prévoit également l'obligation de diligenter des audits internes ou externes sur le respect des obligations énoncées.

Aussi, on pourrait imaginer le renforcement des exigences relatives à la finalité du traitement. En ce sens, le principe de minimalisation des données peut être l'instrument adéquat. Maître Alain Bensoussan estime à ce sujet qu'un responsable de traitement n'est pas obligé de connaître ou reconnaître.

Ainsi, il semble possible que la prévention de la vie privée soit possible dans le contexte du Big Data.

Pour aller plus loin, le défaut de loyauté sanctionné par l'article 226-18 du Code pénal qui dispose que « *Le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende* » peut être considéré comme un moyen de se prémunir contre toute dérive

potentielle d'un traitement de type Big Data. Selon Alain Bensoussan, le principe de loyauté permettrait en outre de contraindre le responsable du traitement de révéler à la personne l'ensemble des données comportementales qu'il détient sur elle. Cependant, il est encore trop tôt pour se prononcer sur l'efficience du droit d'accès dans le paradigme du Big Data.

Conclusion

Rien n'est donc établi en ce qui concerne l'anonymat sur Internet et cette étude est vouée à vieillir rapidement vu la croissance extrêmement véloce su réseau Internet. Nous tendons en effet vers une société dans laquelle l'information sera parmi les plus précieuses des valeur, qu'elle soit personnelle, politique, sociale ou économique.

L'étude de l'anonymat comme principe préventif des atteintes à la vie privée et à l'intégrité de l'identité des personnes souffre du même désintéressement que la plupart de personnes éprouvent pour certains droits pourtant considérés comme sacrés. Le droit de vote est à ce titre l'exemple le plus criant : jamais l'abstention n'a été aussi forte. Pourtant, que se passerai-t-il si demain nous n'avions plus le droit d'élire nos représentant ?

Faire un tel parallèle entre vie numérique et démocratie est d'autant plus pertinent qu'aujourd'hui, la règlementation visant à protéger les données personnelles est en débat au Parlement Européen. Le récent scandale sur la surveillance qu'opèrent les services secrets américains sur nos contenus laissent pourtant espérer un regain d'intérêt pour ces questions qui touchent à nos chers droits de l'homme.

Que l'ingérence dans nos vie soit le faits des administrations étatiques ou des forces économiques, il est impératif de ne pas se vider de notre essence humain en adoptant une attitude trop passive ou trop complaisante. La faculté de pouvoir exercer nos droits est un privilège et toute limite imposée au respect de la vie privé ou à l'identité doit être discutée et mesurée.

Par ailleurs, il n'en va pas seulement des libertés des personnes. La croissance de l'économie sur Internet et de l'économie des données repose avant tout sur la confiance que les internautes ont dans leurs interactions numérique. L'anonymat sur Internet est un droit que nous avons par défaut avant tout traitement. C'est un principe. Nous acceptons très facilement l'identification qui constitue l'exception de ce principe. Cette exception, suivant les services, est plus ou moins envahissante et risque à tout moment de rompre la ligne rouge de l'intrusion et de briser ainsi la relation de confiance.

Pourquoi ne pas revenir à un Internet émancipateur et permettant le développement de notre personnalité ou bien d'autres personnalités ? La pédagogie des usages d'Internet devra un jour faire son entrée dans les programmes scolaires.

Pour Daniel Kaplan, « *la projection de soi inclut la protection ; pas l'inverse*. »[149] Cette idée implique d'établir des relations symétriques entre le bloc constitué des régulateurs et des opérateurs économiques et celui constitué par la société civile numérique. Nous avons le devoir de revendiquer sans cesse la transparence et le respect du droit justement car Internet nous permet de le faire.

[149] Daniel KAPLAN, *Informatique, libertés, identités*, Editions FYP, 2010, p.132.

Bibliographie

Ouvrages

- Guillaume DESGENS-PASANAU, Eric FREYSSINET, *L'identité à l'ère du numérique*, 2009, Dalloz.

- Fabrice ROCHELANDET, *Economie des données personnelles*, La Découverte, 2010.

- Fabrice Mattatia, *Traitement des données personnelles*, Eyrolles, 2013.

- Daniel KAPLAN, *Informatique, libertés, identités*, Editions FYP, 2010.

- Jérôme HUET, Emmanuel DREYER, *Droit de la communication numérique*, LGDJ, 2011.

- Ludovic PAILLER, *Les réseaux sociaux sur internet et le droit au respect de la vie privée*, Larcier, 2012.

- Guillaume DESGENS-PASANAU, *La protection des données à caractère personnel, La loi informatique et libertés*, LexisNexis, 2012.

Articles juridiques

- Lawrence LESSIG, « Code is law, On liberty in cyberspace », Harvard magazine, jan.-fév. 2000.

- P. DE CANDE, « La responsabilité des intermédiaires de l'internet ou ISP : l'apport du projet de loi sur la société de l'information », *D.* 2001, chron., p. 1934.

- J. R. REIDENBERG, « L'affaire Yahoo ! Et la démocratisation internationale », *CCE* 2001, étude n° 12.

- Olivier ITEANU, « Droit à l'oubli numérique, hétéronymat et cassoulet », Iteanu Blog, 19 fév. 2010.

- Irène BOUHADANA, « Constitution et droit à l'oubli numérique : état des lieux et perspectives », Revue de l'Institut du monde et du développement, Les éditions IMODEV, 2011

- Anthony BEM, « Consécration des droits à l'oubli et à l'anonymisation des décisions de justice sur Internet », Legavox.fr, 12 oct. 2011, consulté le 12 mai 2013.

Articles de presse

- Dom BOCHEL GUEGUAN, « Morano et l'anonymat sur Twitter : une nouvelle polémique pour rester dans la lumière », Le Nouvel Observateur, 5 juin 2012.

- Julien L., « La justice sud-coréenne juge l'anonymat indispensable à la liberté d'expression », Numerama, 24 août 2012, consulté le 12/05/2013.

- Ben ROONEY, « The debate over online anonymity », *Tech-europe, The Wall Street Journal*, 17 jan. 2013.

- Hubert GUILLAUD, « La valeur sociale de la vie privée », Internet Actu, 21 octobre 2009.

- Hubert GUILLAUD, « De la valeur du pseudonymat aux dangers de l'identité réelle unifiée », InternetActu, 25 jan. 2012.

- Hubert GUILLAUD, « Big Data : nouvelle étape dans l'informatisation du monde », InternetActu, 14 mai 2013.

- Thomas SAINT-AUBIN, « Design your privacy : pour une licence de partage des données personnelles », Internet Actu, 22 juin 2012.

- Renaud HONORE, « Le Parlement européen enterre définitivement ACTA », Les Echos, 5 juil. 2012.

- Renaud HONORE, « PRISM : Bruxelles demande des explications à Washington », Les Echos, 11 juin 2013.

- Damien LELOUP, « Le Parlement européen vote contre le traité anticontrefaçon ACTA », Le Monde, 4 juil. 2012.

- Xavier BERNE, « Après SOPA et PIPA, la menace CISPA », PC Impact, 6 avr. 2012.

- Julien L., « L'anonymat des blogueurs une nouvelle fois sur la sellette », Numerama, 27 fév. 2013.

- Alfred KOBSA, « Privacy-Enhanced Personalization », Communications of the ACM, 2007.

- Guénaël PEPIN, « La police japonaise recommande le blocage du réseau TOR », Le Monde, 23 avr. 2013.

Actes juridiques

Droit international

- Déclaration universelle des droits de l'homme du 10 décembre 1948.

- Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales

- Comité des ministres du Conseil de l'Europe sur la protection de la vie privée sur Internet, Annexe de la recommandation N° R (99) 5, 23 février 1999.

- Conseil de l'Europe, Comité des ministres, *Recommandation du Comité des Ministres aux Etats membres sur la protection des droits de l'homme dans le cadre des services de réseaux sociaux*, CM/rec(2012)4, 4 avril 2012

Droit de l'Union européenne

- *Charte des droits fondamentaux de l'Union européenne*, 2000/C 364/01, 7 décembre 2000.

- *Directive du Parlement européen et du Conseil relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur* (« *directive sur le commerce électronique* »), 8 juin 2000, 2000/31/CE.

- *Directive sur la protection de la vie privée dans le secteur des communications électroniques*, 12 juillet 2002, 2002/58/CE.

- *Directive relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données*, 24 octobre 1995, 95/46/CE.

Droit interne

- Constitution du 4 octobre 1958.

- Déclaration des droits de l'homme et du citoyen du 26 août 1789.

- *Code civil*

- *Code pénal*

- *Code de la propriété intellectuelle*

- *Code des postes et des communications électroniques*

- *Code de l'action sociale et des familles*

- *Loi pour la confiance en l'économie numérique*, n°2004-575, 24 juin 2004.

- *Loi relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers*, n° 006-64, 23 jan. 2006.

- *Loi relative à l'informatique, aux fichiers et aux libertés*, n° 78-17, 6 jan. 1978

- *Loi du 29 juillet 1881 sur la liberté de la presse.*

- *Loi relative à la liberté de communication*, n° 86-1067, 30 septembre 1986.

- *Loi favorisant la diffusion et la protection de la création sur internet*, n° 2009-669, 12 juin 2009.

- *Loi favorisant la diffusion et la protection de la création sur internet*, n° 2009-669, 12 juin 2009.

- *Loi relative à la protection pénale de la propriété littéraire et artistique sur internet*, n° 2009-1311, 28 octobre 2009.

- *Décret relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne*, n°2011-219, 25 février 2011.

- *Décret relatif au traitement automatisé de données à caractère personnel autorisé par l'article L. 331-29 du code de la propriété intellectuelle dénommé « Système de gestion des mesures pour la protection des œuvres sur internet »*, n° 2010-236, 5 mars 2010.

Divers

- *Proposition règlement relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données),* 2012/0011 (COD), 25 jan. 2012.

- Groupe de travail TIC, *Déclaration des droits de l'homme numérique*, Mairie d'Issy-les-Moulineaux, Livre blanc d'André SANTINI et d'Alain BENSOUSSAN, 20 novembre 2000.

- Groupe international de travail sur la protection des données personnelles dans les télécommunications, *Report and guidance on privacy in social networks services* (Rapport et orientations sur la vie privée sur les réseaux sociaux) ou « *Rome Memorandum* », 4 mars 2008, 675.36.5

- CNIL, « L'adresse IP est une donnée à caractère personnel pour l'ensemble des CNIL. européennes », 2 août 2007.

- CNIL, « Marketing ciblé sur internet : vos données ont de la valeur », 26 mars 2009.

- Groupe « Article 29 », *Avis sur le concept de données à caractère personnel*, 20 juin 2007.

- Groupe « Article 29 », *Avis 5/2009 sur les réseaux sociaux en ligne*, WP 163, 12 juin 2009.

- Groupe « Article 29 », *Recommandation 3/97, L'anonymat sur Internet*, WP 6, 3 décembre 1997.

- Groupe « Article 29 », *Avis sur le concept de données à caractère personnel*, 20 juin 2007.

- Groupe de travail TIC, *Déclaration des droits de l'homme numérique*, Mairie d'Issy-les-Moulineaux, Livre blanc d'André SANTINI et d'Alain BENSOUSSAN, 20 novembre 2000.

- Groupe international de travail sur la protection des données dans les télécommunications, *Privacy by Design and Smart Metering : Minimize Personal Information to Maintain Privacy*, 675.43.18, 12-13 sept. 2011.

- Yves DETRAIGNE, Anne-Marie ESCOFFIER, *La vie privée à l'heure des mémoires numériques. Pour une confiance renforcée entre citoyens et société de l'information*, Rapport d'information n°441 (2008-2009), 27 mai 2009.

- *Proposition de loi tendant à faciliter l'identification des éditeurs de sites de communication en ligne et en particulier des « blogueurs » professionnels et non professionnels*, n° 423, 3 mai 2010.

Glossaire

Big Data : Traitements d'une somme massive de données qui se caractérise par le volume etrêment important des données traitées, la variété de ces données ainsi que la vélocité du traitement. L'analyse de données à travers un processus Big Data est assurée dans un but prédictif (de comportements, de faits sociaux, politiques ou économiques).

Cloud computing : ou *informatique dans les nuages*. Forme de gérance informatique qui repose sur un nuage de plusieurs ordinateurs. En général, les caractéristiques techniques du nuage ne sont pas connues du consommateur.

Cookies : ou *témoins de connexion*. Petit fichier envoyer par un poste serveur vers un poste client afin d'être reconnu lors des prochaines connexions.

Hétéronymat : utilisation de plusieurs identités alternatives, distinctes de l'identité civile, par une seule et même personne.

Mémoire cache : ou *antémémoire*. C'est une mémoire qui enregistre temporairement des copies de données provenant d'une autre source de donnée, afin de diminuer le temps d'accès (en lecture ou en écriture) d'un matériel informatique (en général, un processeur) à ces données.

***Opt in* :** Option d'adhésion, se dit d'un fichier de données personnelles dans lequel un internaute ne peut être inscrit que s'il exprime explicitement son consentement.

***Opt out* :** Option de retrait, se dit d'un fichier de données personnelles dans lequel un internaute est inscrit sans son accord et continue de figurer tant qu'il n'a pas explicitement exprimé son refus.

Privacy by design : Principe selon lequel le respect de la vie privée commence dès la conception des machines. Les règles de protection de la vie privée sont par exemples traduites en lignes de code ou algorithmes.

Tag : Balise accompagnant un flux de données sur un réseau informatique afin d'en préciser l'adressage. Un tag peut être apposé sur un contenu texte, photo, vidéo ou audio. Sur Twitter, on parle de *hashtag* (on place alors le symbole « # » en guise de balise).

Index

Table de jurisprudences

Jurisprudence européenne

CEDH

- CEDH, 4 décembre 2008, n° 30562/04 et 30562/04, *S. et Marper c. Royaume-Uni.*

- CEDH, 13 février 2003, n° 42326/98, *Odièvre c. France.*

CJCE/CJUE

- CJCE, 12 nov. 1969, aff. 29/69, *Erich Stauder c. Ville d'Ulm.*

Jurisprudence de droit interne

Décisions du Conseil Constitutionnel

- Cons. const., 27 juil. 1982, n° 82-141 DC, *Loi sur la communication audiovisuelle.*

- Cons. const., 23 juill. 1999, n° 99-416 DC, *Loi portant création d'une couverture maladie universelle*.

- Cons. const., 10 juin 2009, n° 2009-580 DC, *Loi favorisant la diffusion et la protection de la création sur interne.*

- Cons. const., 10 mars 2011, n° 2011-625 DC, *Loi d'orientation et de programmation pour la performance de la sécurité intérieure.*

- Cons. Const., 29 juillet 2004, n° 2004-499 DC, *Loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.*

Décisions des juridictions suprêmes

- CE, sect., 19 oct. 2011, *French Data Network*, n° 339279.

- CE, 17 juin 1932, *Ville de Castelnaudary*, Lebon p. 595, concl. JOSSE.

- Civ. 1re, 19 juin 1961, D. 1961. 544 ; JCP 1961. II. 12298.

- Crim., 17 nov. 1992, Bull. crim., n° 379.

- Crim., 27 oct. 1999, n° 98-86.017, Bull. crim., n° 235.

- Crim., 7 oct. 1992, n° 91-12.845.

- Crim., 4 et 16 janvier 1974, JCP 1974, II 17731.

Décisions du fond

- TGI Bobigny, 14 décembre 2006, *Laurent F. c/ Sacem et autres.*

- TGI Paris, ord. , 24 décembre 2007, *Techland c/ France Telecom et autres.*

- CA Paris 13ème chambre, section B, 27 avril 2007, *G. c/ Ministère Public.*

- CA Paris 13ème chambre, section A, 15 mai 2007, *S. c/ Ministère Public et autres.*

- TGI Paris, Ch. 1 sect. 1, 22 octobre 1997.

- TGI Paris, ord. de référé, 24 janvier 2013.

- TGI de Paris, ord. de référé, 14 avril 2008, *Bénédicte S / Google Inc., Google France.*

- TGI de Paris, ord. deréféré, 19 octobre 2006, *Mme H.P. c/ Google France.*

Délibérations CNIL

- CNIL, *Délibération portant recommandation sur la diffusion de données personnelles sur internet par les banques de données de jurisprudence*, n° 01-057, 29 novembre 2001.

- CNIL, *Délibération de la formation restreinte prononçant une sanction pécuniaire et une injonction de cessation de traitement à l'encontre de l'association LEXEEK*, n°2011-238, 12 juillet 2011.

Jurisprudences étrangères

- Louis BRANDEIS, 4 juin 1928, *Olmstead c. Etats-Unis (Olmstead v. United-States).*

- Tribunal fédéral allemand, 15 déc. 1983, *Volksählungsgesetz*, BverfGE 65, 1, 41.

Table des matières